Volume Twenty-Nine, Number Three
Autumn 2012, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

7 25274 83158 6 23>

Payphones of the Arab World

United Arab Emirates. This brightly colored phone was seen in Abu Dhabi where even the trash manages to be color coordinated. This phone only takes cards.

Photo by DrJeep

Egypt. People in Alexandria have the choice of using the red handset or the blue one. It has absolutely nothing to do with *The Matrix* nor with rising up against oppressors and eventually winning. But there do seem to be more red ones.

Photo by 1188

Libya. This phone was found in Green Square in Tripoli, where there's still a bit of cleaning up to do. The booth itself is mostly used for posting political campaign ads while the inside does a pretty good job as a trash receptacle. If you're looking for a handset here, you'll have a tough time.

Photos by Tony Anastasio

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

PLAYLIST

The Eyes Have It 4

Technology at the Federal Bureau of Prisons 6

Using Bluetooth Devices as an Additional Security Measure in Linux 10

Hackers Indispensable for Volunteer Groups 12

TELECOM INFORMER 13

The Quadcopter Crash Course 15

Spear Phishing at a Bank - A Hard Lesson Learned 18

Restoring Honest Elections 20

Hackers In Space 21

Hacking Apple's System 24

Fundamental Flaws in Online and Phone Ordering 25

HACKER PERSPECTIVE 26

Beware the Cyber Weapons Industrial Complex 29

XML Automated Gambling 32

LETTERS 34

Stuxnet: An Analysis 48

How to Leech from Spotify 50

TRANSMISSIONS 52

Radio Redux 54

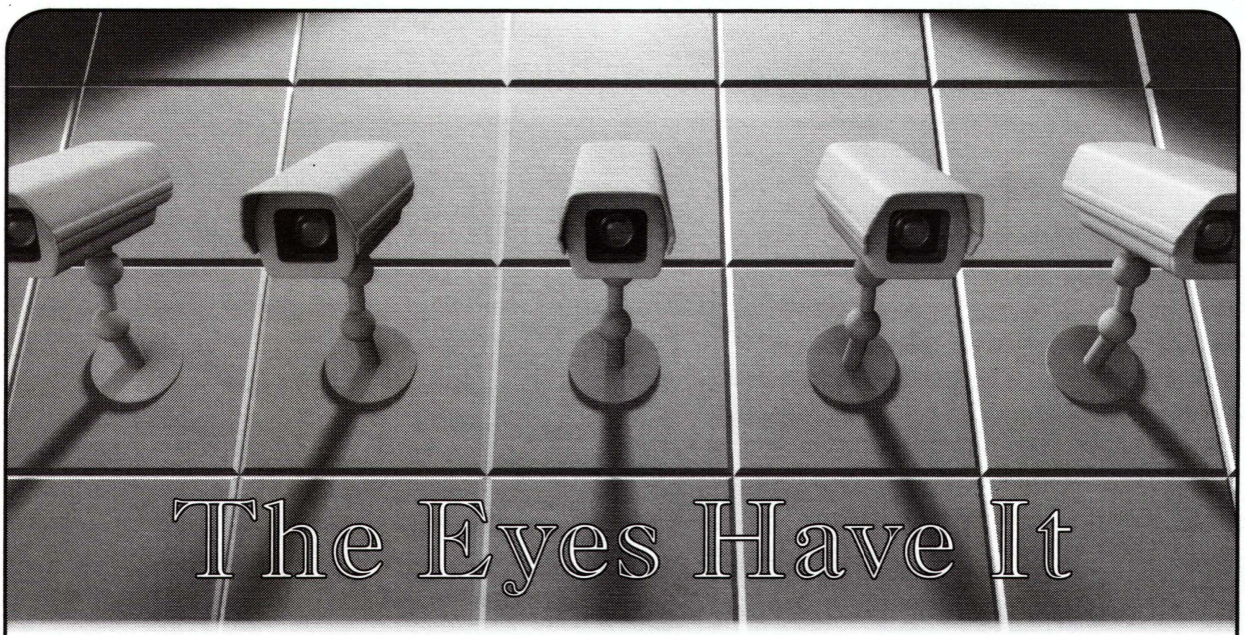
Physical Security Threat from Hotel WiFi 59

A Nice, Hot, Socially Engineered Meal 60

HACKER HAPPENINGS 61

MARKETPLACE 62

MEETINGS 66



The Eyes Have It

Our first warning of the dangers of surveillance came early: our debut issue of January 1984, where we reported on tracking devices that were being installed in Hong Kong automobiles for the purpose of charging for road use. It was even reported that street cameras were being programmed to snap a photo of the license plate of any car whose driver attempted to tamper with the device. Orwellian, to say the least.

Today, congestion charging is commonplace, we willingly add devices to our cars that can play back the routes we've taken, and we're especially eager to install theft protection that will locate our missing autos, should they fall victim to a car snatching. And, of course, street cameras are everywhere.

As a society, we spend an awful lot of time focusing on the advantages of these gadgets and not enough on the potential threats they pose. Sure, we protect the environment by tracking and taxing frequent drivers. But we're also setting up the ability to *always* know where a vehicle is or has been. And that is a definite threat to anyone who still values privacy.

License plate scanners can quickly find cars with outstanding tickets - or the general location of someone who's wanted for one crime or another. Or really, *anyone* whose whereabouts are of interest. And, like most surveillance of today, there's no way to know when you're of interest.

Devices like LoJack are great for finding stolen vehicles. But it doesn't stop there. Who wouldn't also want that ability for their lost pet or abducted child? Whether it's a device inside a car or a chip under the skin, it's capable of working anytime, not just when you need it. But we've convinced ourselves that the world is such a dangerous place that the risk of abuse is a necessary tradeoff.

Cameras on streets have gotten so popular among the frightened populace that some neighborhoods fight to have more installed in order to battle crime. However, there is no clear evidence that these devices do anything to *stop* crime, and, in fact, they've been shown to simply encourage criminals to find a camera-free zone to do their dirty work. In cities like London, even that might be difficult, as it's practically impossible *not* to be on camera if you're walking around town. But the city is no safer than it was, based on its own statistics. And yet, people remain convinced that constant surveillance is a necessity.

In addition to the steady increase of surveillance over time, our very notion of what constitutes surveillance has changed. We raised the warning years ago about the dangers of Caller ID, where people would know who was calling them before they picked up the phone. Today, most of us can't imagine what it would be like *not* to have this feature, and any hint that this is somehow a privacy invasion is roundly scoffed at. But calling people without sending your name and number used to be the norm and this form of anonymity wasn't seen as a negative thing at all. It made receiving phone calls somewhat mysterious and even intriguing. And there was much resistance when it started to change. But, like so many other things,

our perceptions of the world around us have changed. We must always be asking if these changes are for the better.

Whether it's by using social networks and apps to constantly let everyone know where we are and what we're doing, or by installing tracking devices of various sorts to always keep us company, we reinforce the belief that it's a normal part of life and that there's absolutely nothing wrong with it. Those who don't buy into it are by default a little more suspicious and might actually be seen as having something to hide. While it hasn't gotten to the point where you can be questioned for not having a tracking implant or for failing to check in with Foursquare, it doesn't take much imagination to see where we might be going if our world perception continues to evolve in this direction. Add a little fear into the mix and a population can be manipulated into doing most anything to protect themselves. Fear, after all, has always been a very effective marketing tool.

But there is one constant value that has remained, despite being increasingly chipped away at: anonymity, which is *essential* in a free world. Yet, every year, the cry of opposition to this notion seems a little stronger. After all, terrorists, child pornographers, and those people who leak information - they all rely on being anonymous, don't they? Our emotions are tweaked to the point where we feel that anything must be done to stop these people, even if it means giving up something we once prized, even if precious little factual information accompanies our emotions.

The value of anonymous email and net activity has always been high on the list in the hacker community. If the mass media were to get a hold of the previous sentence, you would no doubt be told that hackers (and others) are drawn to anonymity because it facilitates crime. Nothing could be further from the truth. Anonymity has to do with protecting the identity of everyone - from whistleblowers to crime victims to people who just want to be able to speak their minds without fear of retribution. Yes, it can be used for evil as well as for good, but that can be said of *any* element of freedom. If you have trouble envisioning the importance of anonymity in your own world, imagine its necessity in places where freedom isn't held in high esteem and where even visiting the wrong website can get your door kicked in. Fixating on the potential criminal applications is yet another way of giving up something valuable due to fear. It's so very easy to fall into this trap.

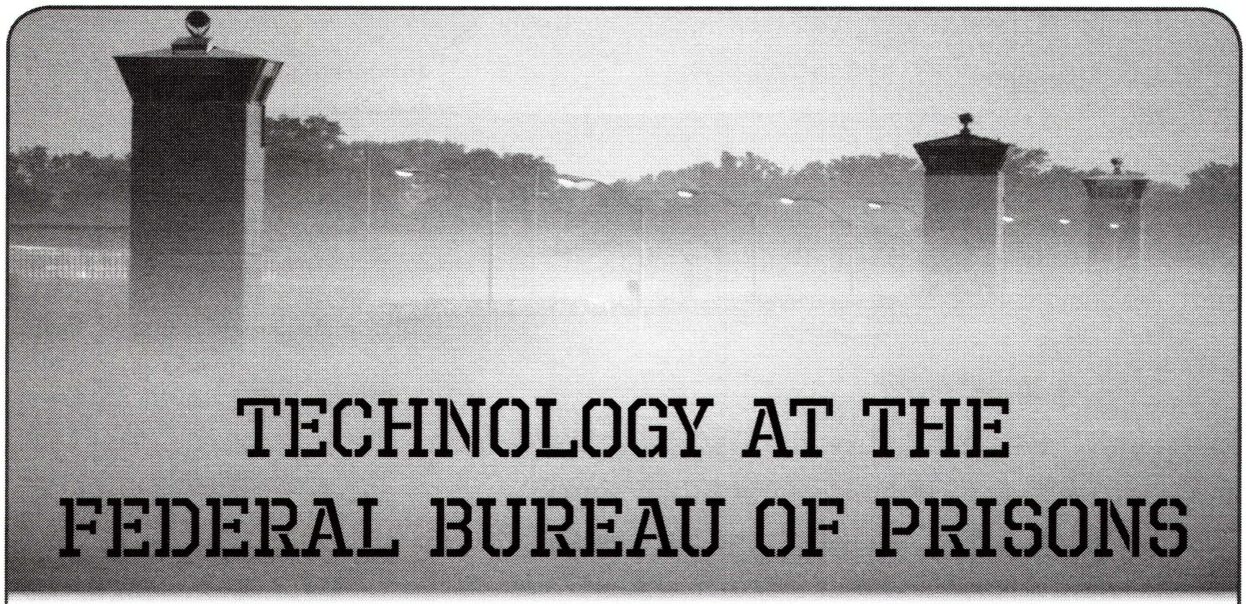
But whether it's through fear or the simple desire to stay connected, we are steadily moving into a world where our whereabouts are always known, our words and actions always tied to our identity. For those who like this sort of thing, there are all kinds of neat and fun things to do with the technology. But at some point, we all have the need to *not* have our presence known, to speak anonymously, to enjoy a bit of privacy like so many used to on a more regular basis. Building a world where this is difficult or looked down upon is a guarantee that our love affair with surveillance will end badly when we realize that we can't escape it.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2012. Annual subscription price $24.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	31688	32250
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	3591	3579
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	27002	27516
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	30593	31095
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	148	145
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	947	1010
E. Total free distribution	1095	1155
F. Total distribution	31688	32250
G. Copies not distributed	0	0
H. Total	31688	32250
I. Percent Paid	97	96

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.



TECHNOLOGY AT THE FEDERAL BUREAU OF PRISONS

by [Name Withheld]

Disclaimer: This article is for entertainment/educational purposes only. Any resemblance to actual persons, computers, locations and/or events is purely incidental. No computers were harmed in the writing of this article.

I'm nearing the end of a 210 month conspiracy sentence in federal prison and I thought I would let the readers know about the computer situation here. It should be similar at other institutions. For those of you who don't know, BOP stands for (Federal) Bureau of Prisons or, if you prefer, Backwards on Purpose.

As a side note, your magazine has been blacklisted here. As with all of the other places I have been, it's allowed for a couple of years until the wrong person notices one of the covers and it scares them. They then get turned over to Computer Services, where it is summarily banned. Novel ideas and freethinking individuals are what they fear the most. I have personally spoken to several of the officers who would have the authority to accept or reject it. Their only response as to why is to say, "It would violate the security and orderly operations of this facility." The funny thing is that a copy of an article will make it in, as will the books.

In the library are five workstations and one print station, each of which is connected to a switch and server in a small rack inside of a cage closed with a padlock. There is an access panel attached with screws. It's a good thing no one here has access to screwdrivers, right? This is in turn connected to a computer room located in the Administrative Corridor. From there it goes to the main server room in the Administration Complex at the main prison. The workstations are Pentium Dual CPU 2.2Ghz E2200 Dells with 1Gb of 800mhz DDR2 running Windows XP.

This is one of the smaller camps in the BOP, so other locations may have more. Other prisons also have them in the housing units. Each one is secured inside of a steel case with a special, rubber coated, TRULINCS branded lock. There are openings for the normal KVM cables, Ethernet, and the power cords. There is no access to the power switch, but the cords are plugged into standard, six outlet power strips screwed to the bottoms of the tables. The computers automatically reboot in case of "power failures." The boot process begins at 5:45 am, seven days a week. The BIOS and setup menus can easily be accessed with a keystroke. There is a password, but....

The computers boot to a login screen where you must enter three numbers to gain access: your eight digit inmate ID number; a nine digit Personal Access Code (PAC number), and a four digit PIN. Our ID numbers are printed on the fronts of each and every piece of clothing issued by the BOP, while the PIN and PAC numbers are written on a piece of paper and given out during the mail call. If a person doesn't attend it, someone else, hopefully without malicious intent, will gather your mail and give it to you.

Normal hours of operation are from 6:00 am until 3:30 pm and then from 4:00 pm until 10:00 pm. If you try to login at an undesignated time, it displays a "TRULINCS is not currently available" message. After three failed attempts to log in, your account is disabled until the administrator re-enables it, sometimes days later. DOS anyone? All keystrokes are captured by the program and do not get passed on to the OS - no

three finger salutes, no Ctrl or Alt key combos, and no Windows key. Another thing to notice is the number on the bottom right of the screen, now 52. I'm assuming it is the current version number as it is incremented during most of the scheduled outages.

Once you are logged into the system, the first screen that appears is the Warning/Responsibilities/Acknowledgment page. You are being monitored. This computer is to be used for authorized purposes only. Don't be bad. Yadda, yadda, yadda. You must "accept" this to continue.

TRULINCS

This computer system is known as TRULINCS (Trust Fund Limited Inmate Computer System). While you're here, it is your bank, library, address book, and email provider. Once you have accepted the terms, the next screen appears. You will see several buttons: `Purchase TRU-Units`, `Public Messaging`, `Print`, `Account Transactions`, `Bulletin Board`, `Contact List`, `Law Library`, `Manage Funds`, `Music`, `Prescription Refills`, `Request to Staff`, and `Survey`. Not all buttons are available on all computers. You can get more info from `http://www.bop.gov/inmate_programs/trulincs_faq.jsp`.

TRU-Units

TRU-Units are credits that can be purchased for five cents each in increments of 40, 100, 200, 300, and 600. There are currently two pay services which use these: `Public Messaging` and Print. E-mail costs one unit per minute and printing is three per page.

Corrlinks

Email is provided by a company named Corrlinks. There is a four-step process to get a contact approved. First, the address is compared to a blacklist. For instance, I was not allowed to write to eyespymag.com about an issue with my subscription. If they are not on this list, they will receive an email from `info@corrlinks.com`, informing them that an inmate wishes to contact them. It contains an eight digit code, good for ten days, which they must use when setting up their account. A link takes them to the site. The site uses CAPTCHAS to discourage the use of bots.

Once their account has been created, a notice appears on the TRULINCS screen in blue saying "you have new or approved contacts." The final step is to contact the person. Contact must be initiated by the inmate. After that, either party may write. Each inmate's address is in the form `xxxxxxxx@inmatemessage.com`. Replace the Xs with the inmate ID number. The person must log into the site each time to check for messages from or to write to the inmate(s). There is a checkbox which can be clicked to have the site send an email notification to you each time you receive a message, but you still must login to read it. There is a 13,000 character limit. No html formatting or graphics are allowed, nor are attachments accepted. All messages over 60 days old are deleted, or so they say. You are allowed one hour before you are kicked off and must wait 30 minutes between logins.

Once logged in, you are free to enter and exit the email as often as you wish, until your hour is complete. Why is this important? From the time you click the `Public Messaging` button until you exit, you are being charged. Whether reading, composing, or replying, it doesn't matter. But it charges only for full minutes used. Therefore, if one were to exit before their next full minute elapsed, that partial minute would be free (though one credit is automatically deducted as soon as you enter the Messaging Center).

There is no cutting, copying, or pasting allowed. More than one recipient can be selected from your contact list. There is also no forwarding, but there is a workaround. Select the message that you wish to forward and click reply. You can then choose a different name from your list.

There is an approximately one hour delay for both incoming and outgoing emails. They are held in a queue, keyword searched, and sent out in batches.

Print

There are two printers: one for regular paper and another for labels, which are required on all outgoing correspondence. Both are located in cages, but the top is open so we can remove our printouts (or access any of the front panel buttons). The only thing the cages are good for is to block us from refilling the paper without calling a staff member with a key (unless one tilted it up in the overly large space and filled it that way).

The `Print` button is disabled on all of the machines except for the Print Station. When

something is printed from one of the regular computers, it is placed into the Print Station's queue. You must then log into it and send it on to the printer.

Labels can be printed for free, up to a limit of five per day. Although, if one were so inclined, they could just use a typewriter and a blank label. Though not exact, they seem to pass inspection pretty well.

GoPrint

Previously, printing was done using a touchscreen, mouse, and card reader/writer which was attached to the server located in the unattended library, and used a program called GoPrint. As with a lot of the full screen interfaces such as this one, there is a way to escape it. A quick double tap in the upper left corner would bring up a window and login screen for the Print Manager.

If this was a new setup, I would guess admin/admin or something similar, but every IT guy knows the first thing one should do is to change all of the default passwords to more secure ones, especially in a place such as this, right? Wrong! A few pokes at the on-screen keyboard and voila, the administrative panel, where one could change the price (lower, free, negative?), the number of copies, etc. Did I mention a card write? Saving the settings and exiting would drop you onto the Windows desktop logged in as the sysadmin. Enough said.

Credits were purchased at the commissary and stored on your ID card. Later, they switched over to a disposable prepaid card - $6.50 for 50 pages - which was also used in the copiers. To make a copy, you first had to insert the card. The reader would display the number of remaining credits and, if empty, eject it.

After the copy button was pressed and your print job complete, the credit was then subtracted. The keyword here is "then." If one were to eject their card prior to the completion of the job, free copies for everyone.

Several of the copiers' functions required a password and it was set, albeit a six digit numeric one. I won't even tell you what it was. If you can't guess it in under a minute, you really aren't trying.

Account Transactions/TRUFACS

TRUFACS (Trust Fund Accounting and Commissary System) is the name of the system that contains the inmate accounts. The `Account Transactions` button allows one to view all of their transactions. This screen has four tabs: the first for your TRUFACS (commissary) account, the second for your TRUFONE and ITS credits, the third for your TRULINCS TRU-Units, and the final one for media. It is not currently used here, but will contain a list of the songs we have purchased for our MP3 players, not yet available at all locations. Fraunhofer and Thomson will be smiling with a quarter million potential, new customers. Anyone heard of OGG?

The FBOP has gone biometric. To make purchases at the commissary, you must provide them with a thumbprint. The reader doesn't work very well and it sometimes takes several tries to accept it, and not always correctly.

Bulletin Board

This is where notices, announcements, schedules, call-outs, menus, etc. are posted. Call-outs are lists of inmates names and numbers telling where they need to go at a certain time, and their bunk numbers. Identity theft and regular theft are just two of the concerns here. One thing of note that I encountered here is the TRULINCS Training Manual. In its explanation of how to use the Bulletin Board, there is a screenshot of a document not normally available for our perusal - an instruction manual for a Citel IP phone C4110. Interesting.

Contact List

Here is where we add our contacts. Every person with whom you wish to communicate, whether by email, snail mail, or telephone must be listed. The required fields include: the first and last names, relation (family, friend, clergy, business, etc.), country, zip code (which automatically fills in the city and state fields), and address. The street is chosen from a dropdown populated with all available choices. Additional fields include telephone number, email address, re: and comment. None of these are verified in any way whatsoever.

Certain addresses are not allowed, such as the address of the institution. They don't want us to waste labels by printing return addresses for the envelopes, or to give to our families to use to write to us. If you need a label with a banned address, there is a checkbox next to the street field that says "My street does not appear in the list." If you check it, it adds another dropdown where you can select a letter to narrow your selection down. Choose any one. It doesn't matter. Another checkbox will appear saying "My street still doesn't appear in the

list." Check it and you can type in any address you desire, even if it was the one that wasn't allowed before.

Law Library

Two of the computers are designated Electronic Law Library (ELL) computers. These allow local access to the LexisNexis database, updated every month or so, where we can research legal matters. We used to also have American Jurisprudence (AmJur), but it has been removed. It was by far the most phun of the two. It allowed "bookmarks" to be placed in the files. These were intended to be a link to a text file where you were taking notes or pictures of evidence or audio that would be opened in the proper viewer. Can you see where this is going? What would happen if an executable were linked to the program? Possibilities were endless.

One could also go to the `File Open` menu and browse for other "books" to open. An interesting place to search was the "users" folder. This is when we still had Windows logins rather than TRULINCS. Our usernames were our inmate ID numbers and the default password was test@1234567. Most people never used their accounts and could easily have been pwned. The users folder contained the numbers of every inmate who was able to use the system. But there was one that really stuck out: 77777777. What could the password be? It turned out that this was an account created by the sysadmin that he could copy whenever a new arrival came and needed an account. There were also others called test and printl. Take a guess at their passwords. Go ahead, I'll wait. I haven't really used LexisNexis enough to say much about it.

Manage Funds

This button allows you to send money to one of your contacts, or set some aside for your release. The checks go out in a week or two and look like normal government checks. I'm sure you can see the potential for trouble here.

Miscellaneous

The remaining four buttons are grayed out and aren't being used yet. Music will allow us to purchase songs, supposedly from walmart.com, but that has yet to be confirmed. `Prescription Refills`, `Request to Staff`, and `Survey` need no explanation.

TRUFONE/ITS

The Inmate Telephone System deserves an article unto itself, but I'll cover it briefly here. The phones are Set Tel Inmate V7006 GBK black boxes made by Wintel. They are pretty basic looking. The current ones are black. The blue ones were removed a year or so ago. There is a red plaque mounted in the upper left corner of the booth that warns you that you are being monitored. The monitoring is done by the staff. They have the ability to log into any of the staff computers and pull up a recording of the calls. There may also be a computer listening for keywords to flag the call for staff review. A big flag is speaking a foreign language besides Spanish. Each phone has a small metal plate riveted to the upper right of the box containing a four digit number, numbered sequentially.

The current version of ITS uses voice recognition. To initially record your voice you must dial 111 and then your PAC number. You are asked to repeat your name three times, then it is played back for you. To hear it again, dial 112 followed by your PAC number. 113 and your PAC number allows you to transfer money from your TRULINCS to your TRUFONE account.

An interesting number to dial is 116. It reads off two numbers, then hangs up, The first number is the same on all of the phones here. The second one is different on each phone, but they are in sequence with the numbers on the plates, though not the same.

To place a call, local or long distance, just dial the ten digit number. For collect calls, you must first dial 0. For international callers, you must dial 011, then the number. Of course, each of these must be followed by your PAC number and saying your name. Prices for local calls are seven cents, long distance 23 cents, and international is around a dollar.

Conclusion

The FBOP should rethink their password policies or actually follow them. They should rethink their IT department hiring policies - being able to walk and chew tobacco at the same time does not a good employee make. Security by obscurity does not work with inquisitive minds. There are many things that should be changed and some that have. Though our bodies may not be free, our minds are - free to learn, to explore, to resist. Hack the world!

Using Bluetooth Devices as an Additional Security Measure in Linux

by Aaron Grothe
ajgrothe@yahoo.com

BlueProximity is a program that can be added to your Linux system to have your system perform actions automatically when a Bluetooth device is in or out of range. BlueProximity does this by monitoring a paired Bluetooth device and performing a set of actions when the device is no longer available.

Disclaimer: it is possible to spoof Bluetooth addresses, so this is not a foolproof system. It can be useful as part of a defense in depth strategy.

To use BlueProximity, you'll need the following:

- Bluetooth adapter either built into your machine or a USB device. DealExtreme has a USB Bluetooth adapter that works really well with Linux that costs less than $2.00 shipped
- Bluetooth device. Lots of people will select their phones. Keep in mind that cheap Bluetooth headsets can also work quite well for this purpose and they won't drain the battery on your phone
- Bluetooth stack/management software installed on your computer - if you install BlueProximity with your package manager on your system, this should be installed along with the BlueProximity software
- BlueProximity software - Installed through your computer's software manager

Getting Started

First, you will need to pair your Bluetooth device with your Linux computer. This is usually done through one of the following programs: Bluemon, BlueDevil or Gnome-Bluetooth. After the device is paired, you can go to the BlueProximity icon, which should be displayed on your toolbar, and start configuring it. All you have to do initially is select a Bluetooth device to monitor and accept the defaults. By default, the system will lock the screen when you are typically more than 25 feet away and unlock when you get closer than that.

To quickly get the system to kill all of your ssh connections, change the line for the locking command from `gnome-screensaver-command -l` to `gnome-screensaver-command -l && killall ssh`. You can chain commands together with `&&` to have the lock/unlock actions do multiple commands for you.

Potential Uses

Out of the box, BlueProximity will automatically lock your computer's screen when your Bluetooth device is unavailable. Don't worry, you can always enter your password to unlock the screen saver.

Ideally, you can have it perform actions like the following as well:

- unmount encrypted filesystems so they are not available on the system
- kill your dropbox session
- portknock a remote system to let it know you are locking your system
- run a program like wipe on sensitive files
- kill ssh connections to remote machines
- almost anything else you can think of

A Couple of Quick Tips

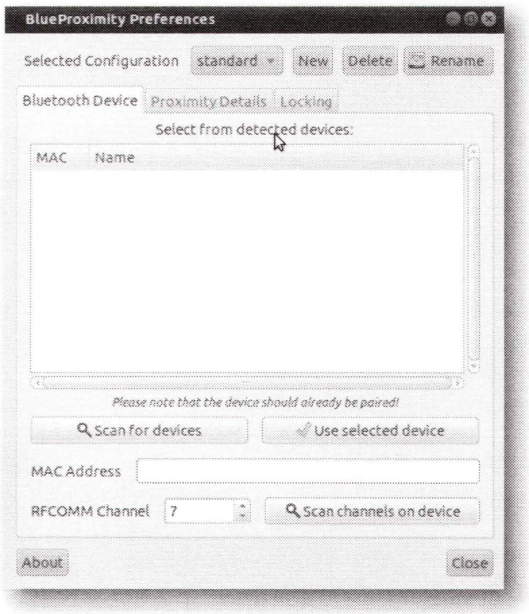
Do not set the lockout duration to zero - there will be occasional hiccups in the Bluetooth communication and this will help prevent you from hitting random locks.

If you right-click on the BlueProximity icon, you can select pause which can be helpful when playing around with the settings.

To have the system do multiple tasks, you can either use `&&` or `;` between the commands to have the locking/unlocking actions perform multiple tasks.

To have the system do more complex tasks, replace the commands in the Action commands section with scripts. That way, you can do multiple tasks easily.

Make sure the device is paired with your computer before you use it. If you don't do this, you might hit random locks as the Bluetooth device might not stay available if not paired.



Links

- *Deal Extreme* - Incredibly cheap USB Bluetooth adapters that work well with Linux - http://www.dealextreme.com/p/super-mini-bluetooth-2-0-adapter-dongle-vista-compatible-11866
- *BlueProximity home page* - http://blueproximity.sourceforge.net - not usually needed as most distributions offer BlueProximity through their package repositories
- *Bluemon home page* - http://www.matthew.ath.cx/projects/bluemon - not graphical, but is more powerful in some ways as it can be set up to do multiple items easily
- *BTProximity* - http://www.daventa.com/products/btproximity - similar program for Microsoft Windows Vista/7
- *Proximity* - http://code.google.com/p/reduxcomputing-proximity - similar program for Mac OS X

WE WANT YOU TO WRITE FOR 2600!

Write for *2600* and help shape the hacker world! From the beginning, our articles have been written by people of all ages, backgrounds, and opinions. We speak with many voices and yours can be one of them. Is there something involving technology that fascinates you? Do you have some tricks you'd like to share? There are so many topics where thinking like a hacker can make all the difference in making things work better, getting around restrictions, coming up with brand new ideas...

So please send us your submissions and keep *2600* fresh. (We'll give you free stuff in exchange.) Your article can be of any length but they generally run from 500 to 3000 words depending on detail. Be sure that your entries aren't online or otherwise printed.

(Anonymity respected and protected when requested)

articles@2600.com

or

2600 Articles
PO Box 99
Middle Island, NY 11953 USA

Hackers Indispensable for Volunteer Groups

by markb

In the low-budget, not-for-profit world, hacking is a necessity. I live in a small, sub-arctic community and I belong to three local community groups and one provincial group. Staff members are mostly volunteers and, in their roles with the groups, they focus on their group's mission and not the technology that makes the gears turn. Computers are donated clunkers that usually arrive broken and/or infected (why else would the owner give it away). The Internet modem comes with WEP-encrypted wireless and a dumbed-down inteface that locks out features. Websites have forums that become toilets. Charger cords fizzle out or disappear and a new one is $300 (if available). A motherboard capacitor is smoked. A scanner has a 25 pin DIN connector. Etc., ad-infinitum, etc.

There are a hundred of these low-budget community groups within any given population of 200,000 persons. None of them has an IT department or a soldering iron.

There is a solution.

There are 30 or so willing hackers within any given population of 200,000 persons: people who like to learn, play, and solve problems, and who have a useful level of creative ability, pattern recognition skill, research aptitude, and a tenacious refusal to be beaten by limitations.

It's a lot of time, though. Computers in the group office and laptops in the volunteers' laps are the most time consuming. Once the solder has been applied, the memory replaced, the BIOS re-flashed, and an OS installed, the work (fun) begins. For example, our community's nature lodge has a computer that is used by visitors and volunteers to view presentations, search the web, use web mail, etc. The network also has an IP camera that is focused on the bird feeder and is available on the Internet. The camera is also accessed by a program on the computer that captures images when motion is detected. The network is exposed to the Internet (for the IP camera, updates by ssh, and remote desktop).

It is used by random persons with unpredictable skills and caution levels. Visitors/staff don't want to develop new computer skills at the lodge and they will ignore admonitions on sticky notes attached to the monitor. They will install tool bars, delete system files, navigate to fake anti-virus sites, download offensive materials, bookmark malware sites, etc. "Help," they say every week, "I can't get my files." Managing a system like this can be a time consuming headache, even for a hacker. Volunteer computer managers often have to "fix" the machine on each visit... never really knowing what problems they may have missed. As always, there is a mitigating hack using a template virtual machine.

A (VBox) virtual machine is inherently restorable and can be comprehensively backed up. We use fresh-daily clones from a stable virtual machine template. We use Linux for our native OS and run Windows in a virtual machine (but you can use this approach if your VM is Linux or if your host is Windows). In a startup script, a clone of a template virtual machine is made each morning. The previous day's clone is erased just before each new clone is made (new tool bars and 100 dirty pictures vaporized). Daily permanent storage for users is done with a thumb drive (a weak point if the drive is infected). Is this a hack? I think it is because it generalizes the VM concept in a such a way that it controls the entropy of a stochastic and dynamic system... volunteer community group computers.

There is only about one willing hacker for every three small non-profits. He/she is very busy. Even periodic updates for a dozen or so computers will use your gas money and keep you in a deserted group office at 1:00 am (instead of home in front of your computer). Enter ssh. But wait, the VM guest is Windows, so I'll need Remote Desktop. Humm, I'll tunnel RDP over ssh. But wait, I'll need to get to the host too, so I can overwrite the template. Humm, I'll ssh into my Linux host too, perhaps using a VNC tunnel. I wonder how I can port forward my virtual NAT adapter rather than giving access to my LAN through the VM? How will I conveniently manage and use 15 ssh connections/keys from my home computer? Any one of these elements has a discoverable tab-and-slot workout, but making them all sing together requires "critical thinking, creativity, inquisitiveness, problem solving skills, and a hunger for knowledge." (ternarybit, *2600,* 29:1, page 26)

What's the point of all of this? As I read my issues of *2600,* I often recognize an undertone of concern with the "optics" of hackerdom. We know we're (mostly) good, but some think we're evil. Volunteer, non-profit groups from 4H to the Women's Federation provide essential services: social, environmental, educational, etc. For every dollar they socially engineer from funders, they generate ten dollars of service (usually, anyway). In our "electronic/information" age, they are enabled by hackers. So, when your boss asks, "What are you doing with that hacker magazine on your desk?" show them this page.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! We just finished a rainy summer here in Beijing, in which some of the biggest floods in more than 60 years occurred. This resulted in some rather exciting conditions for the Central Office that challenged our original engineering assumptions, since we never expected to need high-powered sump pumps and Noah's Ark in the parking lot. The net result is that I'm now in for another long, cold Beijing winter, since it looks like I'll now be here until February. At least it's so cold that it'll snow instead of rain. Of course, we didn't engineer for more than 12 feet of snow, so I'd better be careful what I wish for!

Meanwhile in the United States, something incredible happened over the summer: hacker-operated GSM networks sprang up at hacker events all over the country! At HOPE, the Telephreak crew built a network that was available on the vendor floor. At Defcon, the Ninjas (disclaimer: I am one of the Ninjas) ran a "NinjaTel" network that operated inside the conference area of the Rio, and they gave away Android-based HTC phones with some really cool custom Ninja software. And at ToorCamp, a Seattle-based group of phreaks called ShadyTel built a fully licensed network with an incredible range, covering the entire camp. You could build one too! The technology has reached the point where serious geeks and hobbyists are able (although I won't claim easily able) to create their own GSM networks.

At the most basic level, to build a GSM network, you need four components:

- *Base Transceiver Station (BTS):* The radio transceiver that communicates with mobile phones and devices
- *Base Station Controller (BSC):* Controls the BTS and interfaces it to the Mobile Switching Center (MSC)
- *Mobile Switching Center (MSC):* The MSC is a switch. It routes calls locally or to the public switched telephone network (PSTN).
- *Visitor Location Register (VLR):* Generally a function provided by the MSC, the VLR is responsible for authenticating devices with the Home Location Register (HLR) and granting access to the network.

Building a BTS

The most popular platform for experimenting with building a BTS is called OpenBTS. When paired with an Ettis Research Universal Software Radio Peripheral (USRP) programmable hobbyist radio and a software tool called GNU Radio, OpenBTS effectively turns it into a BSC. The Ninjas believe that this is the only reasonably cheap, nonproprietary solution currently available, and they used it for their implementation.

There are a couple of disadvantages to using USRP and OpenBTS. GSM is a pretty tight specification from a radio perspective, and USRP devices are difficult to tune precisely. Also, OpenBTS only supports seven voice channels and one data channel. NinjaTel used a version of OpenBTS called openbts-multi-arfcn, which is a release that supports additional capacity. Note that OpenBTS is an open source application, but the hobbyists who created it also maintain a commercial branch offering additional functionality through their company Range Networks.

An alternative to USRP radios which are under development but not currently ready is an open source hardware design called UMTRX. When it ships, it is expected to cost under $700.

OpenBTS isn't the only option. Another open source BTS implementation is called OpenBSC. This is designed to work with a limited number of commercial GSM base stations. Why limited? Theoretically, it should work on any base station because the protocol, ABIS, should be standardized. Unfortunately, as often happens in the technology industry, vendors have varying (and incompatible) interpretations of the specification, so only a limited number of devices actually work with OpenBSC. Until recently, commercial BSC hardware was relatively complicated and expensive to obtain. However, the large number of carriers upgrading to 3G and 4G BSC units has resulted in a glut of used 2G GSM kits. ShadyTel took advantage of low prices, large inventories, and no questions asked. Accordingly, they were somehow able to inexpensively purchase Nokia Insite microcells, which are supported by OpenBSC. These are typically used to cover indoor areas such as shopping malls, and they work on standard 120v utility power. However, they work nicely outdoors as well. The advantage of using purpose-built GSM base stations is that they are specifically designed for use with GSM handsets, and have better performance. OpenBSC is also more scalable (by default) than OpenBTS, which is another reason why ShadyTel preferred to use it.

Unlike the garden-variety Ethernet interface

available on USRP radios, commercial BTS equipment comes with a variety of interfaces. Unfortunately, none of these are particularly standard on PCs. The Nokia Insite microcells that ShadyTel used have an E1 interface (E1 is the European flavor of a T1). Fortunately, E1 line cards for PCs are readily available on eBay for about $100, so ShadyTel bought one of these and they were in business.

Whether you're using OpenBTS or OpenBSC for your BTS, you'll need to decide which frequencies to use. Unfortunately, using any frequency commonly used by GSM worldwide (frequencies in the 850, 900, 1800, and 1900MHz ranges) requires a license in the U.S. Fortunately, for low power applications, licenses are available from the FCC for only $60! For their ToorCamp deployment, ShadyTel obtained a Special Temporary Authority (STA) license from the FCC to transmit on the 1900MHz frequency range. It took about three months to obtain the license, so planning ahead is advised.

VoIP MSC

Obviously, the next piece is the MSC. Both OpenBTS and OpenBSC are designed to work with Asterisk, an incredibly versatile soft PBX platform. An MSC isn't the only necessary piece of the network (note that a VLR is also required), so a MySQL database is used to provide this. Asterisk can already act as a full-fledged switch, offering nearly infinite opportunity to customize. NinjaTel offered far and away the most customizations, offering voice prompts recorded by Pat Fleet (the "voice of AT&T"), a replica of the Defcon conference bridge, a time service, and much more. ShadyTel, for its part, offered full-blown connectivity worldwide via VoIP (which hackers used to great delight, running up a whopping $22 bill with the SIP provider). None of the three networks at hacker events opened their networks to roamers; all required their own SIM cards to register. Oddly enough, every group purchased their SIM cards from China. The most interesting SIM cards were those obtained by ShadyTel. They are Java-capable SIM cards that run custom applications, allow the carrier to modify numbers dialed by the subscriber, and more.

Lessons Learned

Every network experienced challenges - even when really smart hackers build it, it's pretty hard to make a pop-up GSM network run well! Telephreak and NinjaTel experienced difficulty with the hostile radio environment of a hacker event. Too many people were walking around with cellular jammers, and these took their toll on the networks. NinjaTel also relied on the Defcon wireless network to deliver a significant amount of the functionality built into their Android-based operating system, but the network proved less reliable than they hoped. Exacerbating the problem, NinjaTel experienced a hardware failure on their USRP BTS, resulting in a significant loss of transmitting power for several hours until repairs were made. ShadyTel, meanwhile, planned that their equipment cabinet would be located in a cabin. At the last minute they were given a portable toilet instead, so they needed to re-engineer their equipment rack to fit inside. As it turns out, portable toilets are really well insulated! They retain heat well, and this is exactly the opposite of what you want when you're running equipment that needs to be cooled. The Asterisk server then overheated repeatedly causing the network to "crap out."

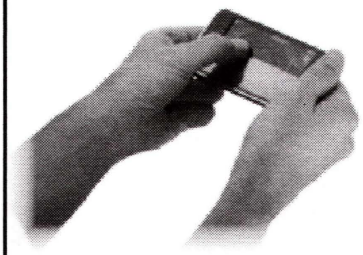
Future Possibilities - And a Warning

One of the biggest vulnerabilities of the GSM protocol is that the designers never contemplated the possibility of malicious base stations. As Chris Paget demonstrated at Defcon in 2010, it's relatively trivial to spoof a base station and disable GSM encryption. Two years ago, it required a big antenna and a lot of bulky equipment, but we're now not far away from being able to fit everything needed to run a GSM network with a half-mile range into a backpack. Like most technological innovations, this is a double-edged sword. Although you can't trust the security of 2G GSM anymore, this also means that it could become relatively easy for dissidents in various countries to work around shutdowns of cellular towers.

There is much more to explore about this topic than I have space for in this column, so if you're curious about building your own GSM network, I hope you'll go online to learn more! The possibilities are really infinite and I hope to see hackers and tinkerers everywhere playing with this stuff. Please check out the references below, and have a phun autumn!

Phun References

- http://en.wikipedia.org/wiki➥/NinjaTel_Van - NinjaTel detailed description and press article links
- https://github.com/ninjanetworks - Android source code used for NinjaTel
- http://www.shadytel.com - ShadyTel
- http://shop.shadytel.com - Leftover Java-enabled smart cards and readers not used at ToorCamp are available from ShadyTel at a low cost
- http://www.telephreak.org - Telephreak
- http://wush.net/trac/rangepublic - OpenBTS wiki
- http://openbsc.osmocom.org/trac➥/wiki/OpenBSC -OpenBSC wiki
- http://gnuradio.org/redmine➥/projects/gnuradio/wiki - GNU Radio wiki
- http://transition.fcc.gov/pshs➥/services/sta.html - FCC Special Temporary Authority information and application
- http://patfleet.com - Pat Fleet, the Voice of AT&T



The Quadcopter Crash Course

by UAVman aka DeathNinja McSex
UAVme.wordpress.com

Before I start on what is to be a massive purge of all knowledge I have gained in my obsession-fueled journey, I have to state that that journey was inspired entirely from watching this video: `www.youtube.com/➥watch?v=fyYujjP5J-k`. After watching, I instantly had the urge to build one and hope that by inviting as many people as possible to view it, I can infect more people with this obsession as (from my perspective) it is a healthy obsession, being that it's hard to do this while sitting in a basement, doesn't involve any "victims," and has the real chance of you coming into direct contact with sunlight, which can only be a good thing (no offense to the basement dwelling folk, but this gave me a good excuse to get out of my own basement and cure my rickets, at least until I had to add more stuff to it). It doesn't take too long before venturing back into that space people call "outside" to test the latest editions, lest your neighbors think you're inventing some kind of insane sex toy in the basement).

As the title suggests, this article is aimed at anyone who isn't already familiar with the subset of UAVs and remote controlled vehicles called quadcopters (or multirotors or hexacopters as they are also called), and is not a guide on how to crash your contraption. It is intended to outline underlying principles that one should be familiar with when delving into the bewildering yet rewarding endeavor of crafting a quadcopter.

First things first. What is a quadcopter? To put it as succinctly as I can, a quadcopter is a remote controlled or Unmanned Aerial Vehicle that achieves lift via fixed propellers facing skyward. Usually four or more of them are mounted on a frame at equal distances from the center of the vehicle. It is stabilized by equal amounts of torque from rotating and counter-rotating motors which are matched and mounted opposite each other (counter-rotating motor opposite counter-rotating motor and so on), aided by a flight control board. Creating a difference in that torque balance rotates the vehicle. Creating differences in speed between pairs angles the vehicle along that pair's axis. Controlling speed of all motors at the same time via the throttle controls the overall altitude of the vehicle. Using a combination of these options controls the vehicle similar to a helicopter (roll, pitch, and yaw), albeit with a lot more agility.

For those already bitten by the quadcopter bug looking for a pricey shortcut, there are more than a few outfits willing to part you from your hard earned (or ill-gotten) cash in exchange for some impressive kit. Prices range from a few hundred to a few thousand, and some even more so. But in my opinion, you'd be paying to take all the fun out of it.

There are a couple ready to fly. One such product is called the AR Parrot. A Linux powered, iPhone controlled quad that sells for between $250-$400 depending on where you get it from. If this is your cup of tea, then it's time to fire up Google and ready your wallet. But, fair warning: there isn't much room for upgrades, although I'm not gonna argue against hacking it. You may also have seen one at your local Radio Shack (or Jaycar as is the equivalent down here in Australia) branded as a UFO or something similar. Again, fair warning: these are very "cheap" in all senses of the word.

Don't jump on that computer just yet. By the end of this ordeal, Santa himself (or your nearest psycho) will envy your list making

skillz. But to get through this, you will need to make Google your friend (or at least a close acquaintance) and get comfortable with some new info. Before you set off to make that list that you will check at least twice, it's important to know about all the components that make up a flight worthy quad, and the rules of thumb that will guide you along the selection process. So let's begin a breakdown of the common quadcopter setup. (I recommend using as many off-the-shelf parts as possible. Not only is it easier, but it will also save you a lot of time and sanity.)

Electronics You Say...

That's right, you will be dealing with cryptic ratings that describe the electrical properties of the components you're considering. Don't worry bro, I got you. You don't need to be an electronics whiz; there will be no Maxwell's equations or KVL KCL methods. I'm not even going to include any equations because that's just the kind of guy I am. I will, however, give you a few things to remember. First, red means positive, black means negative. Second, an amp is a measurement of electrical pressure referred to as current, as opposed to voltage, which is roughly a measurement of electrical volume. So think of it like you would a river. The voltage would be equivalent to the width and depth of the river and amperage or amps would be the force driving the... ahem current. Really, all you have to remember for this article is what red and black mean and that one amp is equal to 1000 milli-amps, kinda the same as one gigabyte is equal to 1000 megabytes. So now we come to the components you will have to choose.

The Motors

Generally, you need at least four of them, although some have gotten away with three, but you have to use three servos as well. The motors you'll be looking for are called brushless motors of the outrunner type. I'm not going to get into the differences between brushed and brushless or inrunners and outrunners. I'll let you and Google sort that one out. For now, let's just assume that they are best suited for the amount of torque and speed needed. What you want to concern yourself with is the maximum amps they draw and the amount of lift you can achieve with a given propeller size. A good ball-park figure would be 700g+ lift for each motor, providing a total lift capacity of 2.8Kg+ for all four, with a maximum current draw of somewhere between 20-30 amps each for a total of 80-120 amps drawn. Locking these values in will point you in the right direction of the next item you need to search for.

I Feel The Need

Generally referred to as an ESC or electronic speed controller, these are what will drive your motors and manage their speed. This is accomplished with some real electronic voodoo wizardry (well, not really, but a full explanation could very well take up the rest of this article). Suffice to say that connecting your ESC to the motor isn't rocket surgery. There are three corresponding wires on each. Just connect them and if your motor isn't spinning the right way, swap any two wires and it will reverse the direction (there is no wrong way to connect these wires). Generally, you'll want an ESC that can provide a good 10-20 percent more than the maximum amps drawn by the motor, which will help to keep your ESC cool. For instance, if your motor of choice will draw a maximum of 20 amps, you'll want an ESC that is rated at 25-30 amps. You could match it at 20, but if you find you need to push the throttle past 50 percent just to get off the ground, you'll wear those suckers out quick and mid-air failures aren't exactly hot right now. So once you've found your ESCs of choice, you'll have a good idea of what to choose next.

You'll Need Power For That Scotty

That's right, the all important battery. You ain't goin nowhere without one. Willpower can only achieve so much. For the given task of getting you off the ground, the best suited battery is the Li-Po (lithium polymer) battery. They're light and pack a punch. Be warned that Li-Po batteries are the exploding type, meaning that a puncture in the casing (or overcharging/discharging) could mean fire or explosion, so take care when you're using/transporting/charging/handling your battery. Like motors and ESCs, they have cryptic ratings that you'll need to understand. First is the capacity, measured in terms of milli-amp hours or Mah, which means how many hours worth of milli-amps it can provide. For example, a 2000Mah battery can provide 2000 milli-amps for an hour or 1000 milli-amps for two hours, etc. The second is the "C" rating, which refers to the battery's discharge capacity. A battery with a 30C rating will be able to discharge 30 times its capacity in terms of milli-amps. For example, a battery with 2000Mah rated at 30C will be

able to provide 60,000 milli-amps (30 x 2000) or 60 amps (remember, one amp = 1000 milli-amps), and, all things being equal, will run out of power 30 times faster. A good rule of thumb is to give yourself some headroom, like ESCs - 10-20 percent more "C" should mean that you won't overheat or strain your battery. The third rating you need to know about is the nonsensical "S" labeling, which refers to cell count (I'm guessing they made up the "C" label first). This will give you your batteries' operating voltage. One cell = 3.7 volts, two cells = 7.4 volts, three cells = 11.1 volts, and so forth. 1S = one cell, 2S = two cells, etc. From here, you can ascertain what the operating voltage is and choose the right battery for your system. All motors and ESCs operate within a given range of S's, so you'll want to re-factor that into your choice of motor and ESC combos. Generally, most garden variety motors and ESCs operate within ranges of 2-4S, all of which can be sourced at your local hobby store. The only other choices you have to make are whether you want a hard or soft case, and the type of plug to use (if one isn't included, some soldering will be required). I recommend the XT-60 type, personally. It's also recommended that you get a power distribution board. This will connect to your battery and provide an individual connection for each ESC. Most boards will have similar dimensions to a lot of flight control boards and will only need nylon spacers to mount under them and onto the frame.

Where It All Comes Together

For sanity's sake, I urge you to get an off-the-shelf solution as your frame. It will save you a lot of time and possibly blood. The more adventurous or gifted among you might choose to craft their own, but chances are there's a more precise and better looking frame out there that will cost you less than the raw materials it takes to make one from scratch. Having said that, I did make my own, being that there weren't all that many options when I was first consumed by the quadcopter bug, but the flights were brief and crashy, so if you're going to venture down the DIY path, I'll offer some friendly advice, which is applicable to almost all things DIY, and that is "measure twice, cut once" and only where you intend to cut. And if you do end up going to the hospital, bring this issue with you and spare yourself the explanation of what you were doing, and what a quadcopter is.

Control Yourself

The flight control board is the all important brain of your quadcopter and will most likely determine whether it flies or runs away. These boards stabilize your quadcopter by taking the commands from your communication method of choice (generally an RC receiver), mixes them with some clever programming and IMU (Inertial Measurement Unit) measurements, and outputs signals your ESCs understand. There are a myriad of options in this category from the cost effective $20 Atmel based "kkcontroller board" to the professional priced $1,140 "DJI Wookong M - Multicopter AutoPilot with GPS" and a hell of a lot in between. I've personally only used the kkcontroller and AeroQuad boards as Id rather spend my walking around money on my collection of Ferraris and Faberge eggs. I can't honestly give any recommendations apart from what I've personally used. I do recommend the kkcontroller board to those on a budget, but you will need to read the instructions for tweaking. I will include a list (nowhere near complete) of the available board options for you, but it is in no way endorsing them. I'll leave that up to your Googlefoo skillz. They are as follows:

- The "kkcontroller" board from `www.kkmulticopter.com` and also `www.hobbyking.com`
- The Arduino based "AeroQuad" from `www.aeroquadstore.com`
- The "HoverflySPORT" and "HoverflyPRO" from `www.hoverflytech.com`
- The DJI "NAZA" and "Wookong M" from `www.dji-innovations.com`
- The "FC 1212-S Flight controller" from `www.rchobbyhelicopter.com`
- The "OpenPilot CopterControl" platform from `www.openpilot.org`

There are a range of differences between these platforms in terms of tuning options and add-ons. For beginners and newcomers to RC in general, the NAZA seems to get good reviews, but a good and thorough comparison online is the only way to know for sure what will suit your needs and skill level. My only advice is that when spending this type of cash, unless your time is more valuable than these items, I suggest you spend it familiarizing yourself with the options available to you.

Loud and Clear

The other pricey part in this article. The RC transmitter/receiver or RX/TX system. The

latest generation use spread spectrum techniques within the 2.4ghz frequency ranges and cost a bit more than a pretty penny, but are well worth it in the long run. There are el cheapo options from various vendors, but they're tied to a single receiver and have a severely impaired set of options for tweaking control characteristics. That said, if you're on a budget, a $20 cheapo four or five channel TX/RX pair can't be beat, because from there your next price point is somewhere north of $250, although the six channel Spektrum dx6i set can be had with some searching for under $200. Either way, I'll leave it up to your discretion, googlefoo, and your tolerance for half-witted jokes made at the airfield.

Take Charge

One final thing you'll need is a good charger and power supply. You'll also need to invest some time in learning how to use them, and the optimal rates of charge for your battery of choice, generally charging at between 1-5C will save you headaches. But I can't stress the point enough that if you make a mistake here, without the necessary protection, you're putting people's safety at risk, so again "Google it." Most RC battery chargers are designed to take multiple power sources, including your car battery. So you need a power supply for when you retire to your abode. It's a good idea to get a protective charging pouch for your batteries just in case they do decide to explode. Read the instructions for your charger to minimize your chances of this.

It's a Setup

A full assembly guide is way beyond the scope of this article, but I will, however, provide you with enough keywords to feed Google to find your way out of the shit I got you into. First, there are many configurations; what I've described so far are the basic components. From here, you'll need a good idea of what setup is good for your intended purposes. The basic four motor setup can be set up in either a "+" or "X" configuration, meaning that the former will have a single leading motor in any direction of travel while the latter will have two motors. Combine two more motors/ESCs with a hexframe and you can make a hexacopter, which just means you'll have six arms on the frame with two or three leading motors. Get a "Y" frame and you can make up a Y6 configuration consisting of two motors on the end of each arm on the frame (one on top and one on the bottom). Get a further two more motors/ESCs with the right frame and you can make an octocopter, which I'm sure by now you can work out for yourself, or you could make an X8 setup which is like a Y6 but with an extra arm. From here, there are a few more exotic setups but the ones listed are the best supported. Some YouTube searches with your chosen setup, plus a few other keywords like "assembly" and "tutorial" thrown in will come up with some instructional videos. But looking at how the pieces fit together, you should be able to work out what goes where.

Feel free to follow my exploits on my blog at `uavme.wordpress.com`, where I will be posting my own experiences with various combinations, and links to resources and products. If you have any problems, I'll be more than happy to help out or at least point you in the right direction.

Happy flying.

Spear Phishing at a Bank - A Hard Lesson Learned

by lg0p89

This article is for informational purposes only.

I work at a local community bank. The bank is not a big target for security minded individuals and our presence on the net is minor. We sit in our own little corner of the world and don't bother anyone.

An email was sent from our "HR Director." This is a person of authority and senior management in the bank. The email looked legitimate with the correct name, phone extension, and bank logo. All the words were also spelled correctly, as they generally are not with this type of attack.

The body of the email was regarding an updated anti-virus (AV) program. We have all seen this, but the target was clueless. The message was written in lay terms, as the HR Director would write. To the average bank employee, this looked perfectly normal and

not out of the ordinary. After all, with all of the viruses that are present, updates are quite regular and normal. An AVP in the mortgage lending area with a very happy pointer finger clicked on this. Now the story really begins.

This email was not the only one sent to the bank that evening - obviously. It was not a single incident - this was actually much larger. The email was sent to several people in the bank in different departments, not just the mortgage area. The email - although copies of the same email were sent to a number of people - was also selective as to who it was sent to. Thankfully, there was only the one person who was lacking common sense. The direct effect of this was two hours of an IT person, two hours which were greatly needed elsewhere.

There are several reasons she should have been tipped off. First, the HR department does not send out updates for AV programs. For brevity's sake, duh! In the 20+ years of her experience in the bank, each person has never, repeat, *never* had to update their AV. It is all done through the IT department. And last but not least, each system does not have their own individual AV on their own hard drive. Again, duh!

Usually we see the phishing technique at the bank. The typical ones say that you have a UPS shipment waiting and you have to click on "Here" or the shipment will be returned today, or a long lost friend is emailing you and you need to click "Here" for her personal and contact information, etc.

This was a bit more interesting. The sender put more time than the normal amount into this specific attack. This was more of a case of spear phishing. The emails were from the HR director with her spoofed address. This was not from a random person in the bank nor was it a fake employee email. The link in the email was also different for each email sent to the bank employees. The links did not point to the same website. For instance, if four bank employees received the emails, each link in the emails was to a different website.

Due to the formatting, these undoubtedly came from the same person or entity. What is curious is how they could have done this. After all, I (and by extension you) might as well learn from this, versus merely shaking my head and wondering what this employee does instead of thinking.

So how did they do it? I can only give a general theory. I truly and unfortunately (I would like to get more ideas from them) do not know who this is. On the bank's website, there are certain tabs. One tab is "About Us/Annual Report." From this tab, it is only one quick click to download a full copy of the bank's annual report. No, the bank is not publicly traded. Yes, I know. The table of contents lists what page all the employees are listed at. The page, once you turn to it virtually, shows all of the employees' full names and also how many years of service they have to the bank. The annual report does not show the employee email addresses and the email format. This could be easily gathered via getting the HR director's name on the website (this is listed so people may send in their resumes) and also via a generic social engineering request (calling because you need to send a lender an email but you lost his card; can get the lender's name from the annual report freely available on the website). From here the next step is pretty easy with putting the email together and emailing it.

The dangers to the bank are more far-reaching than I care to think about. The email addresses are out there now for future phishing and spear phishing attacks. The person or entity knows this will work. As one of my t-shirts says, "There is no patch for stupid." They know the executive management of the bank due to the bank generously leaving this information for anyone to see. The next time maybe the email will be from the president/CEO. They may send an email to the president of another bank with a file that needs to be opened today, which has malicious code. The link clicked on may also open the bank to a breach of confidential information. Use your imagination as to what types of information and data an enterprising person could get from a bank!

There are a number of lessons hopefully learned - but probably not. There will always be those who refuse to learn from the past and prefer to hold onto old habits. The bank's staff needs to be wary of what information is put out there. The bank, especially a community bank, wants to show itself as being friendly and available to the clients. However, this does need to be balanced, due to the bank not wanting to give out too much information.

There also needs to be more continued training. Within the two months prior to this occurrence, there was a training session on what not to do. One topic was not clicking on strange links. This did not quite sink in, as the resulting issue showed.

And the beat goes on.

RESTORING HONEST ELECTIONS

by Phredd
fredm70@gmail.com

Aside from the fact that America is supposed to be a republic, not a democracy, I was incensed when I first saw the documentary *Hacking Democracy* on YouTube a few years ago. It laid out the numerous ways that elections can be (and have been) hijacked, both electronically and mechanically (i.e., old fashioned ballot box stuffing, disappearing ballots, etc.).

Bev Harris was a grandmother in Washington State who accidentally stumbled upon Diebold's FTP site while surfing the Internet one day. If someone who is as technically illiterate as I am can get the election software, she thought, how much easier would it be for a computer savvy hacker to find it and completely control an election?

This eye-opening experience led her to start the website blackboxvoting.org.

I've personally been in the IT field for 33 years now (that's 21 in hex), and though most of it has been in the mainframe world, I began learning distributed computing (e.g. .net, C#, VB, and Javascript) back in late 2007.

It further ticked me off that any company, like Diebold, can get away with writing and selling software that is proprietary (read secret) that is supposed to do nothing more than count votes and report the results. How hard can that be?

If we were to count paper ballots by hand - not as infeasible a task as it first seems - we wouldn't do it behind closed doors so as to invite suspicion regarding accuracy and honesty. Ideally, it would be an operation much like the kind of restaurants one frequents where the patrons can actually watch their food being prepared, nothing hidden from view.

It's tough to rip off an election when everything is done in plain sight, as it should be.

Furthermore, no election software firm or voting machine manufacturer is accountable to anyone for the integrity of their wares. It is ironic that a majority of the public distrusts government, yet they believe that it can be trusted to administer the periodic selection of its leaders.

I can't imagine a good reason why election software should be proprietary, and decided to write some pseudo code that would accomplish counting votes for an election. It appears below, and may strike you as overly simple. If I've overlooked any requirements of a normal election, I'd be interested in knowing it.

```
For each race...
  Initialize all candidates' totals
  ➥ to zero
  Do until all votes are
counted (whether as they are
cast, or when polls close)
    If vote-is-for-candidate-A,
      Add 1 to candidate-A-total
    Else-If vote-is-for-candidate-B,
      Add 1 to candidate-B-total
    ...etc..., through...
    Else-If vote-is-for-candidate-x,
      Add 1 to candidate-x-total
    End
  End Do
  Report totals
End
```

Granted, this considers neither write-in votes nor unintelligible votes (the ridiculous hanging chad comes to mind), but those could be addressed with equal simplicity.

Problem is, from a free-enterprise capitalist point of view, you can't make money with this code; a six year old could have written it. But such is the need for fair elections; the profit motive is hard to defend in this instance, even if easy in most others.

That covers the way elections ought to go from a software standpoint, I thought. But just for grins, I decided to see how many ways I could think of to manipulate the votes toward a desired outcome. Put another way, if I were an auditor reviewing code for evidence of foul play, what would I be looking for?

Without much effort, the following came to mind:

1. Pre-load the preordained winner's vote count with a nonzero total. This can backfire if the turnout for the other candidates exceeds this number plus his turnout.
2. For every n votes cast for the intended losing candidates, add n+x (where x>1) votes for the predetermined winner's count. This could result in an absolute (rather than

relative) margin of victory of n*x votes. (Think of the childhood game, "one jelly-bean for you, two for me...")

3. Similar to number 2, but multiply n by some factor, e.g. 1.17, to give a relative (rather than absolute) margin, in this case 17 percent.
4. Similar to number 2, but for every vote cast for the intended winner, subtract 1 (or more) from the contenders' counts. This is risky because it can theoretically result in a negative total; whether by this exact method or not, this actually happened to Al Gore in at least one precinct in the 2000 presidential election.
5. Whereas 2, 3, and 4 would manipulate the running totals, one final adjustment could instead be made after all votes have been counted, either adding an absolute (as in 2) or a relative (as in 3) number of votes one time.

There are no doubt other ways I haven't thought of, but you see how easy this is. It's ridiculous. Where I live, it seems every election night, as people are anxiously awaiting the results after polls have closed, the local media will announce, from the central election headquarters where the computers are compiling totals from surrounding precincts, that they are experiencing computer problems. Unknown (and unaccountable) experts come in, survey the situation in whatever mysterious but unquestioned methods they employ, and the reports then convey that it's been fixed...

And this doesn't consider the chain of custody issues where the machines are loaded into the back of a van and driven (by who knows what route, by who knows what driver) to the central election location for final processing. Memory cards can easily be replaced, hacked, etc.

Credit Bev Harris for not just relaying the gloom and doom picture of rigged elections in America, but also providing a variety of remedies to the average citizen to ensure elections are honest. Different things can be done before, during, and after an election to bring about this much needed reform.

Even if I could engineer the next election to seat my favorite candidate in office, I would rather devote the efforts to preventing his dishonest defeat.

HACKERS IN SPACE

by MS3FGX
MS3FGX@gmail.com

While those of us in the United States have managed to fight off large scale Internet censorship in the form of PIPA and SOPA (at least, for the time being), the battle to maintain an individual's unfettered access to the Internet is still raging all over the globe. Is it any wonder? With social networks becoming an increasingly indispensable tool for protesters and freedom fighters, the governments of many foreign countries are looking to actively censor, or even deactivate, the Internet at their discretion.

Now imagine plugging a device about the size of a standard USB WiFi adapter into your computer, setting up an antenna, and being able to receive news and information from orbiting satellites even when you can't get access to the Internet. But instead of these satellites being owned and operated by a government or corporation, imagine they were completely under the control of ordinary citizens. Such a network would be indispensable for combating corrupt governments, organizing rescue operations in areas stricken by natural disasters, and providing information to third world countries that don't have a telecommunications infrastructure. But, can it be done?

At Chaos Communication Camp 2011, a talk was given detailing a "modest" proposal for putting a hacker on the moon by 2034 [1]. While I can't say I am too optimistic about that particular goal (there is some debate if even NASA will be able to get anyone off this rock before then), the first phase of their plan (to build a free and globally accessible satellite communications network) is something completely different. With the rapid commercialization of space transport and operations, it's now possible for a group of individuals, using open source software and hardware, to construct,

launch, and operate their own communications satellite, though certainly not easy.

First Steps

When dealing with hardware intended for space flight, there is no such thing as being over-prepared. Anyone attempting to build a device and accompanying software destined for low Earth orbit (LEO) would be wise to start a bit closer to the surface of the Earth, by way of a high altitude balloon. Using readily available weather balloons, it's possible to send a small payload up to 100,000 feet (30 kilometers). At this altitude, the sky turns black and the temperatures can drop down to nearly -100 F (-73 C), an excellent dress rehearsal for a space mission.

Operating a craft in near-space, generally considered to be anywhere between 65,000 feet (20 kilometers) and 350,000 feet (107 kilometers), demands many of the same design paradigms of a true spacecraft: reliability, redundancy, energy efficiency, thermal protection, mass and dimensional constraints, etc. Operating such a craft would also require the ability to track and effectively communicate with a high altitude object, one of the most important aspects of creating a practical communications network. In fact, the Hackerspace Global Grid [2] is a project dedicated to just that subject, the tracking and identification of satellites via open source software and hardware. You can't talk to something you can't find, so this subject is getting a lot of research and development now in preparation of future projects.

While you'll never construct a global communication network with balloons alone, they may have a future in temporary or emergency networks. The LVL1 hackerspace in Louisville, Kentucky is working on the White Star Balloon [3] project, a self-ballasting weather balloon capable of maintaining its altitude and staying airborne for days at a time. While LVL1's goal with White Star is to send the balloon across the Atlantic Ocean via the jet stream, it's not unreasonable to imagine a similarly designed balloon equipped with some type of propulsion system being able to maintain its position (roughly) over an area for extended periods of time. Being able to place a balloon over a target area for use in communications or even surveillance has some very obvious uses. Incidentally, the U.S. military is currently experimenting with this very concept using manned and unmanned balloons.

Getting into Space

Building a high altitude balloon is certainly a challenge, but not outside the grasp of even a clever high school student. It's a good demonstration, but it's a far cry from building and launching a proper satellite. So what now? How do you actually get something into space if you aren't a world superpower?

Not that long ago, you didn't. It just wasn't happening. But as commercial spaceflight started to emerge as a viable enterprise, a new class of satellite quickly started to gain popularity: the CubeSat [4]. CubeSats are miniature satellites, sometimes referred to as picosats or nanosats, which adhere to specifications written by the California Polytechnic State University and Stanford University. CubeSats are 10x10x10 centimeter cubes with a mass of one kilogram, scalable along one axis up to three cubes. This allows for a satellite (known in this configuration as a 3U CubeSat) with a maximum size of 10x10x30 cm and a maximum mass of three kilograms. The mass and dimensional constraints are tight, but with ever smaller components and manufacturing techniques, it should be within the capabilities of a well equipped hackerspace.

Of course, the next question is: how much does it really cost to build and launch a CubeSat? There are a lot of variables involved here, from the size of the satellite to the orbit it's placed in. A realistic estimate for getting a 1U CubeSat (a single 10x10x10 cm cube) into orbit would likely be around $80,000 to $100,000 USD, though depending on who you talk to, the number can be as low as $40,000. While $100,000 is surely a lot of money for us in the "99 percent," it's not an unreachable goal. Consider that the TikTok [5] project managed to raise $942,578 on Kickstarter... and it's a watchband for the iPod Nano. If the hacker community could raise that much money, a fleet of communication satellites would be well within the budget.

For the hacker on an even tighter budget, Interorbital Systems plans on beginning launches for their "TubeSats" [6] this year. The TubeSat is advertised as "the low-cost alternative to the CubeSat," costing only $8,000 for the construction kit, including the launch. The steep discount does come with a penalty however, as the TubeSat offers only three-quarters the total mass of the 1U CubeSat, and is placed in an orbit which will decay after a month or so. Still, there's something to be said for being able to

build and launch your own personal satellite for the cost of a decent used car.

Ears To The Sky

A lot of people seem to be under the impression that communication with satellites requires a ten foot wide satellite dish and a room full of radios. In reality, you can receive the downlink of low altitude satellites with nothing more than a handheld scanner and a simple "rubber duck" antenna. Naturally, this isn't an ideal solution, and a more permanent installation with motorized high gain antennas would get much better results, but it does give you an idea of what's possible in a pinch.

Another common misconception is that satellite communication requires a license. While transmitting to an orbiting satellite would require an amateur radio license from your government of choice, simply receiving broadcasts on the common satellite bands can be done by anyone with the appropriate equipment. Naturally, this means that communication with our theoretical hacker satellite network would be one-way for unlicensed individuals, but that really isn't a problem. The immediate goal of such a project would be to spread news and information to people who would otherwise be cut off from the world, so in that case it would be enough to receive a downlink of the latest pertinent information. Of course, anyone with the appropriate license and adequate equipment could use the satellite network in a bi-directional fashion as well, so both use cases could be served simultaneously.

With recent advancements in Software Defined Radio (SDR), you don't even need a traditional radio to receive broadcasts anymore. Products like the FUNcube dongle [7] are low cost SDR devices specifically designed for amateur satellite communication. Coming in at under $300 USD and controlled by freely available open source software, SDR devices like this bring satellite communication within reach of even the most modestly funded hackerspaces or groups of individuals. As the market for satellite-oriented SDRs grows, we will see those prices come down even farther; to the point that within a few years, a radio capable of receiving satellite transmissions might not cost much more than WiFi hardware.

Reasonable Expectations

With talk of satellite ground stations and launching home-built spacecraft, it's easy to get carried away. A look at any of the mainstream media coverage of projects like the Hackerspace Global Grid will give you a good idea of how easily the imagination wanders (or runs) when talking about anything to do with space.

The major thing to understand is that nobody is suggesting a "parallel Internet." That was an idea the media glommed onto almost immediately, but it's wildly impractical. Establishing a meaningful TCP/IP connection to an amateur satellite would be a challenge for even a well-equipped ham radio operator, so the idea that this could be a service offered to the masses is out of the question right now.

Most likely, the early versions of a hacker satellite network would only be able to broadcast simple text messages. Think of an orbiting serial terminal, and you'll have a pretty good idea of what's possible. Licensed radio operators with the appropriate equipment could upload the message to be broadcast, and the satellites would then repeat it to anyone who cares to listen until they receive new instructions.

Perhaps not as exciting and glamorous as some people might like, but it's a start. Such a system could be invaluable for individuals whose government censors (or cuts off) their Internet access or in emergency situations.

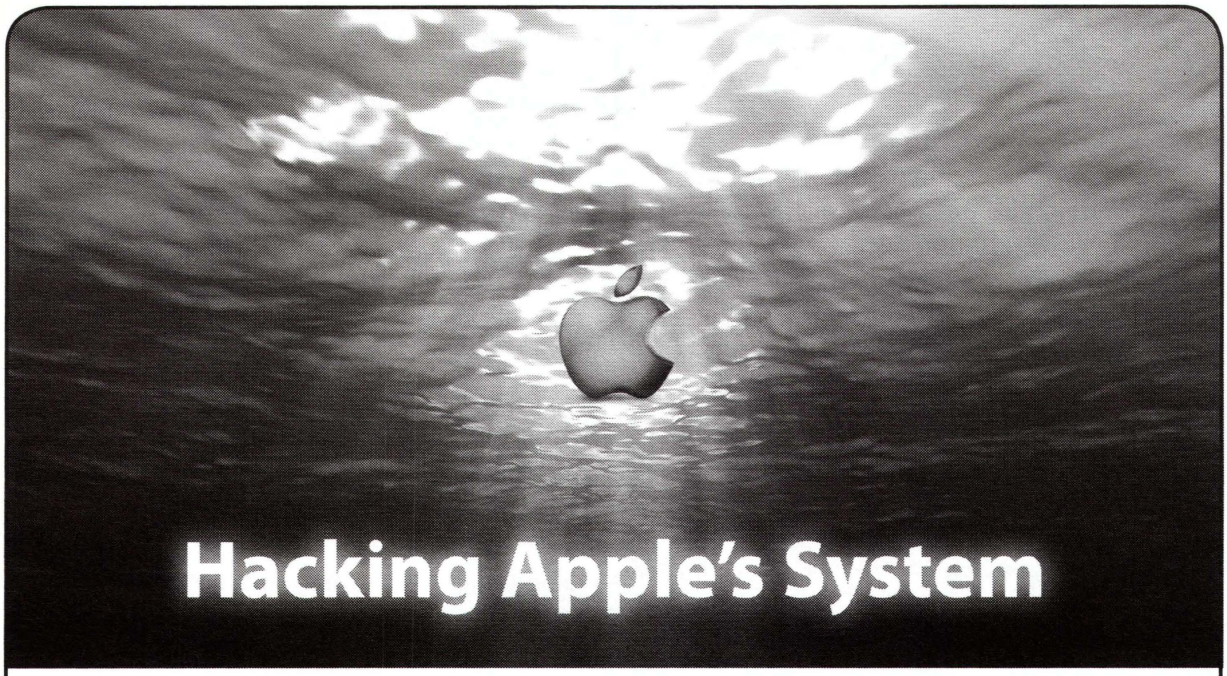
Conclusion

It'll be quite some time before we can surf the web on our own hacker-built satellite ISP. But, with the proper research, funding, and skill, it's not unreasonable to think we could see low cost receivers pulling down data from civilian built satellites within the next two years; assuming there are enough people motivated to make it happen.

As John F. Kennedy said of the Apollo program in 1962, we do these things "not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills."

References

1. http://events.ccc.de/camp/2011/Fahrplan/events/4551.en.html
2. http://www.hgg.aero
3. http://whitestarballoon.com
4. http://www.cubesat.org
5. http://kck.st/al8N3p
6. http://interorbital.com/TubeSat_1.htm
7. http://www.funcubedongle.com



Hacking Apple's System

by Big Bird

First off, I feel it's important to explain that any sort of liquid damage to an Apple product will void your warranty. There has been some talk about an AppleCare+ warranty that covers water damage and cracked screens - but the regular Apple warranty does not. So, I suggest you don't seriously attempt this. What follows, however, is a true story.

As your typical computer-using bloke, I like laptops. I have an Apple Macbook Air. The device is great, and it's light. One day at a local Starbucks, I had just started drinking a coffee when I knocked that grande cup right into the direction of my Macbook. Ack! I was freaking.

The first steps involved turning off the computer and holding down the power button. I flipped the computer upside down and grabbed a bunch of napkins. I kept it upside down with napkins all the way home. Once I got home, the computer went right into a container that held the full Macbook (a bag would work) and I poured all of the rice I had all over the Macbook.

I left that Macbook covered in rice for at least a week, heck, it could have been longer. I didn't touch it, turn it on, or otherwise consider using it. Finally, after the week was up, I attempted to turn it on and the machine booted. I was sad to find out, though, that some of the keys were messed up on the keyboard.

I had to make a choice here: chuck the computer or go to Apple and see what was possible. I decided to ask what the keyboard replacement might cost - and that would be close to $300! Wow. My choice, however loose morally, was to play dumb and see if I could get warranty service.

I first set up an appointment with the Apple "Geniuses." This was a time-of-day appointment that required I simply tell one of the sales guys in the store that I had arrived. When I connected with the Genius, I said to him, "I think my keyboard is broken." Of course, broken keyboards are covered under warranty.

The fellow was nice enough and he tried to remote boot the system by way of a network image to run a diagnostic. Since this was a Macbook Air, he required the use of a network adapter. He wasn't able to get the system to boot. He thought the keyboard was stopping him from that, so he tried an external keyboard to help this process. Failed Again.

It seemed like he was running out of options, so the next thing he did was to take the computer to the back and "check for water damage." The check appeared to be short and it seemed like he might have just pulled the bottom off the case. There is no way in the time he took that he was able to pull the top off. The Macbook Air is not designed to let you in.

So, he came back and said everything was in order and that it would take a week to replace the keyboard and that this would be covered under warranty. Phew. A week later, the computer was fixed, problem solved, and Apple's system was shown to clearly be flawed.

Also of note, Apple recently patented a new form of liquid damage detection. It appears as though they may know that these kinds of warranty services are going on unchecked.

Fundamental Flaws in Online and Phone Ordering

by C P

The place I work takes phone and online orders. Low security leads to high loss.

When a customer places an online order using a cell phone or computer, there apparently is no credit card security code or PayPal limit check. This may be done after the order is submitted, if it goes to a holding pen. This may also happen if the item is unavailable or cannot be delivered as scheduled. No checks are done to determine if the customer's email address and name match, if the customer's phone number is the same as the recipient's, if the customer requested Saturday delivery for something that can't normally be delivered Saturday (FedEx/UPS), and strange messages ("Dear Pamela, You own me now. Fit me up with a radio collar and an invisible fence. Only you and God know how much I needed your text last night. I am deeply committed to you and love you forever. Love from Leslie").

If a customer tries placing an order online more than three or four times, they get an error message to call us for help. If they call, the order may or may not go through, but we won't know until we submit it. If the order doesn't go through, they'll have to use another credit/debit card or try again another day. We can't take cash, checks, gift cards that haven't been registered/don't have security codes, PayPal, more than one promotion (including coupons or points), "free shipping," orders for wine, or orders for personalized items on the phone. If you have a land line and a phone book, you wouldn't know. Everybody else - read the terms and conditions. We aren't lawyers, and telling us you're going to plaster it all over social media won't help you at all.

We have absolutely no way of telling who you are versus who you tell us you are. It doesn't matter if you say you're a Secret Service agent from Albuquerque or a professor from a university in San Francisco whose assistant went missing over the weekend... she's from Germany, and she's so conscientious she'd *never* do that (even if he's supposedly a network security doctoral candidate). It doesn't matter - you still have to get a police report and have the police *fax a subpoena*. That's the way it works. Just do it. Same thing for somebody who calls and says their credit/debit card number was hacked/stolen.

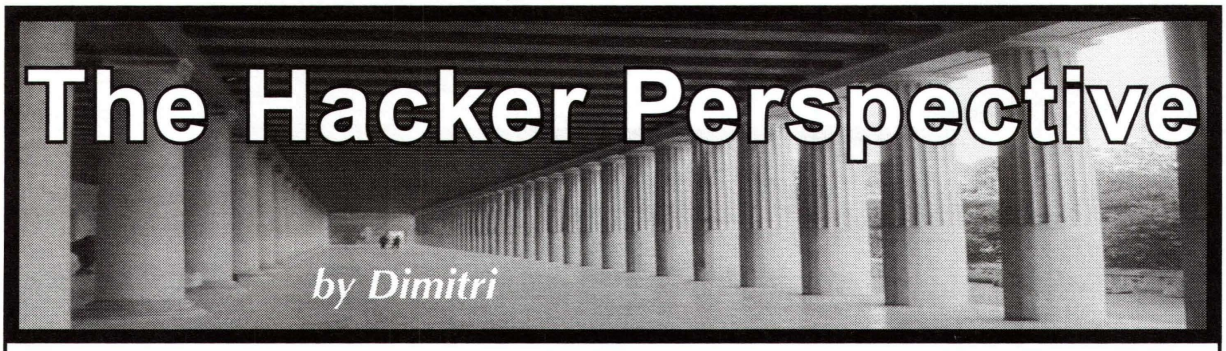
Orders placed through relay operators are usually fraudulent. These calls used to be made by deaf people, not so much now. Have the relay operator ask the caller to give their name, valid billing phone number, billing address, city/state/zip, email address, valid credit/debit card number, expiration date, and security code at the beginning of the call. If J Random Customer can't answer that, the relay operator will tell you "the other party disconnected," or something along those lines.

Phone orders are placed using a JavaScript system running on Internet Explorer 6 on old Dell PCs running Windows XP. No fooling.

Temporary workers are brought in from someplace. Any warm body from off the street apparently will do during major holidays. A couple were fired after they had stuff sent to where they lived (using customers' credit card numbers). Definitely not the sharpest knives in any drawer.

Thanks to all who read this, and thanks to *2600* for this excellent magazine.

The Hacker Perspective



by Dimitri

I'm not famous.

I think that's a good thing. I think generally, if you're a hacker and you have mainstream fame - then something went wrong. I'm trying to avoid things going wrong, but it's harder than it sounds and I've been closer than I'd like. When I see something, anything, I feel I have to know what it's for and how it works, what was it put there for, and how it does what it does.

So I'm a hacker.

I'm not famous, but I don't do it for the fame. I do it because that's the way I'm programmed. But, what do I mean when I say I'm a hacker? I mean that I do things with hardware and software, computers and networks, that the designers didn't expect me to, sometimes didn't want me to.

I don't do it for fame, I don't do it for money, I do it because I see things that other people miss, that they're not able to see and that's exciting. How I can access a network, a whole world that people aren't even aware exists!

So it started when I was younger, around eight - something in the region of 13 years ago. It was never a mainline thing for me, although I now I work as a network engineer, so it's a little more mainline than it was.

When did I start hacking? You'd think that would be an easy question, but it's not, because the line is sort of blurred. The question shouldn't be when did I become a hacker, but when did I notice that I was a hacker?

For me, it was probably around age 11, when I was first restricted. I just wanted to surf the Internet. I was addicted. I researched everything from quantum physics to computer security, constantly. When I got to school, I was first hit by that little warning: "Access to this page has been restricted, as it violates the security policy in place." I got around it. I don't remember exactly how, but it didn't take long. It wasn't difficult.

I didn't want to break the law. At that age, I wasn't even sure what breaking the law was when it came to computer security.

I continued this way for a couple of years, playing on networks and finding networks. I had a very bulky, heavy laptop that I used to carry everywhere with me. If I saw a jack, then I'd plug in - be it a computer network or a phone line - and just see what was out there.

Skip a few more years and I started looking at radio frequencies. I started seeing wireless. By this time, my finances were a little better and I got hold of a handheld. It had a pretty effective 802.11b receiver, so I set it to periodically scan around. Most of the time, I was just looking at the names of the networks as they appeared on my screen to see what was out there. I did a little WarWalking with a GPS receiver and plotted out my local neighborhood. Then I printed it on A3 and posted it on my wall next to a spreadsheet detailing networks that I'd seen.

Kids my age had pictures of movie stars and bands on their walls. I had a statistical analysis of the security systems used by over a thousand companies in my local area. I didn't do it as part of an attack; it wasn't malicious.

I was amazed by the fact that I could see all of these networks and no one else I knew even knew what they were, that they were there, or the security implications of my being not only able to see them, but to access them too. I went from hunting jacks to hunting radio waves.

I openly talked about security. I openly talked about what I saw.

My parents weren't bothered. They didn't understand what I meant. They didn't understand how close I was to the edge of law. I didn't understand how close I was to the law. In fact, it wasn't until I was first questioned that it hit me - that there were restrictions. I knew I couldn't just walk onto someone's property and start going through their personal belongings. Though I had been using a directional antenna from a car park to access a government department's (more than one department, more than once) computer systems and start hunting through not one person's belongings and personal data - but the whole neighborhood's.

When you buy a computer, they don't tell you that you can break the law with it. By the time you realize this, it's too late. Either you're addicted to it already or you're staring at a police officer asking some pretty hard questions about your habits.

You're addicted. Worse, you don't have to the ability to explain what you're addicted to. The police are asking more questions - even harder ones this time - and you don't have the vocabulary to explain what it is that you're doing. Or worse, they don't have the training to understand what you're saying. It gets pretty scary when you can't explain. They're quoting laws and you're quoting frequencies and exploitations. You're not on the same wavelength.

It was fine when it was your parents. They didn't understand, so they just left you to it. It was fine when it was your teachers. Your grades were high, so they just left you to it. When it's the police, it's a different matter. Just hope you're as good at social engineering as you are at network security.

How good can you be, when you're 13? I guess it's all practice. Eight years on, I'm still doing it. I dropped my old laptop and handheld and upgraded, voting for a purely open source operating system, a more powerful machine, and a better wireless card. More power, more speed, more range, more freedom.

My cell prompts me now when it sees something that I might be interested in. I've hooked it up with text-to-speech and it tells me what it sees, and often it even says why I should be bothered. My exploration is automated.

I was walking through town, past a hotel, and I heard a network jump into range. "Network detected: Eee Pee Oh Ess." It happens every now and again. I've heard that network before, I know physically where it's located, I know the kind of encryption it uses, the number of users on at any time of day, and I know what the network is for. EPOS: Electronic Point Of Sale.

I'd heard the network before because I heard it every day on my way into work, though it wasn't until I dug deeper that I realized the implications of having remote access to this system.

If I booted my laptop, I'd see maybe 15 networks. There was the one I was interested in, right in the middle. EPOS. I clicked connect. It asked me for my encryption key. I hit CTRL - ALT - F2 and dropped out of graphics mode and into text-only mode, which is the first step when I mean business. I was wasting CPU cycles by using graphics, and I needed to be quick.

So skip a couple of years. I'm older now. It's a different network. It has a different reason for being interesting to me, but it's the same story. However, this time I know that what I'm doing is illegal, but I don't stop. I've been doing it for years. Why would I stop?

I start capturing packets coming from the network. I see a client and pretend to be it, pretend that I'm authorized. The traffic flows faster and within an hour, I have enough data to calculate the key. It's only WEP. These days, an hour is an age. You can get WEP in 30 seconds, and I can prove it.

Armed with the correct key, I bring my graphics back up and enter when prompted, then watch the icon on my task bar whirl as DHCP is activated and I'm allowed onto the network.

I load some more software now to watch on the wire, capturing data as it passes over the network and I'm watching data bounce around, looking at one machine in particular: "Front-Desk". That looks interesting. I scan it for SMB shares, the kind of network file sharing technology that's used by most home computers. It's got the defaults open, one of which is "C$". A quick dictionary attack gives me access to the whole system.

I'm not really paying attention to what I'm doing. I'm not attacking the network. I'm in autopilot. Something appears on screen that looks interesting, and I start probing and looking at it in more depth.

First, I was attracted by the network's name, then the computer's name, then the known network share, and finally, the last thing that got me on this network: it was running a program made by a company that I recognized.

I couldn't remember what the company did or how they made a profit. I knew I recognized them and there was something interesting about it. It was a software development company specializing in accounting software.

I hit the button to transfer the software and ran some emulation software to allow the code to run on my operating system.

"ENTER ACCESS CODE" appeared on the screen. Four digits. Ten thousand combinations, some more likely than others. 1 - 2 - 3 - 4. Access granted, level ADMINISTRATOR. Surely not.

I wasn't familiar with the software in use on the network, but I'm familiar with how networks work and how machines talk to each other, and how the correct command can get that

machine to do anything that you want. I hit the wrong button, I mistyped a command, I sent the data to the wrong address, or I did it because I wanted to. I wanted to see it happen, to see if I could make it happen. I could - I hit enter.

I was sitting in the hotel lobby and there was a very attractive girl my age, sitting being the front desk. I didn't care about her. I was on their network. That's what I cared about. When I hit that final key, the cash drawer shot open with a crash two feet away from her and she screamed. Everyone looked, and I've never left a hotel faster.

I'm not here doing this because I want to make money, I don't want to be famous. I'm just curious. I'm interested. I'm addicted. Thirteen years after I started, I'm still amazed that people aren't aware of how I do what I do, or what is even possible.

I've been spoken to by the police on more than one occasion and, although I don't set out to break the law, sometimes it happens. I used to talk openly about what I do. Now I don't, though I still hack. I still explore. I still break systems, copy data, and manipulate machines. But I don't do it for personal gain. I never have. I do it because it's the way my brain is wired.

So what's my message? What would I tell the aspiring hacker? I guess I've only got one message.

You don't become a hacker. You're born one.

Submissions for "The Hacker Perspective" are closed for now, as we have enough columns for the next couple of years. But don't fret. Use that time to experiment and learn new things. When we reopen submissions, you will have a lot more to write about! But in the meantime, please send us your articles on other topics. Our mailbox is there for you: **articles@2600.com**

HOPE NUMBER NINE DVDS

The conference is over, but you can relive it (or experience it for the first time) with over 100 hours of DVD footage that captured each and every talk in the main three tracks.

We have way too many DVDs to list here, but we can tell you they're $5 each with a full set running $400 (a savings of $100). See all the details for yourself at **http://store.2600.com/hopenumbernine.html**

We may even have leftover HOPE t-shirts in your size. Check the store for more info.

BEWARE THE CYBER WEAPONS INDUSTRIAL COMPLEX

by Josephus Alexander

In his famous farewell speech, the American President Dwight D. Eisenhower famously spoke about the dangers of the "military industrial complex" and its corrosive power on society (i.e., being a drain of resources from social programs that affect the general well being of the American people via the "defense" budget). Since President Eisenhower's speech in the late 1950s, we can see that his warning fell on deaf ears as defense spending has been increasing while budgets for schools, Social Security, national parks, etc. continue to stagnate or get cut to unsustainable levels.

As the multi-billion dollar military industrial complex continues to sell conventional arms for continuous wars of "peace" against "terrorists," and, of course, "communists," a new aspect of the military industrial complex has arisen out of the depths of cyberspace. This new weapon is not a physical weapon, but a digital one that is not bound by any rules, arms embargoes, or treaties. The effects of this new form of warfare have shown up in Iran in the form of Stuxnet, Duqu, and now Flame. The 20th century saw the building of the military industrial complex, and now the 21st century has spawned its digital successor which we will term the "cyber weapon industrial complex."

Of course before we go further down the rabbit hole, here's the traditional *2600* obligatory disclaimer: This article is for informational and educational use only, so we can all be better informed citizens of the physical and virtual world. Any development of digital weaponry for criminal/terrorist means or being a digital arms dealer (think Nicholas Cage in the movie *Lord of War*) for the above mentioned people is pretty damn illegal and also counts against you for karma and heaven points. Lastly, if you're some government agent at a three letter agency reading this and you start freaking out about the information here, please put your energies somewhere else. All my information comes from those oh so "classified" sources such as Google, my local library, and, of course, the Barnes and Nobles at the local mall. Besides, you guys might want to police up your own backyard in light of the recent disclosures about the American cyber warfare program by *The New York Times* and in a book titled *Confront and Conceal* by David Sanger found in hardcover, audio book, and Kindle. So, with that bit of sarcasm and disdain of over-reactive government officials aside, let's get started, shall we?

Definitions

In order to properly discuss the cyber weapons industrial complex, it is important to define the term and to also talk about the end

product: cyber weapons. So, without further ado, here we go:

- *Cyber Weapons Industrial Complex* - a subset of the larger military industrial complex that produces weaponized/militarized code (cyber weapons) that attacks information systems (i.e., networks, servers, routers, databases, OS, games, etc.) in order to inflict damage or destroy virtual or physical property of a designated enemy
- *Cyber Weapons* (short version because this is an article in and of itself) - computer code (aka botnets, sock puppets, DDoS scripts, viruses, etc.) that is developed or utilized for the destruction of the confidentiality, integrity, and availability of information systems and threatens or causes physical, functional, or mental harm to structures, systems, or living beings

Now that we have defined our two main terms, let's get to know our "friends" in the cyber weapons industrial complex a lot better.

The Purpose

Why build cyber weapons? The better question to ask is really why not? Cyber weapons are a big draw to the customers and the builders of these digital munitions because cyber weapons are relatively cheap (billion dollar stealth bomber and million dollar bunker buster bomb versus a one million dollar Stuxnet virus), readily available (depending on what you want), have a fairly short development cycle, and are for the most part anonymous (unless you run your mouth to a reporter, get snitched on, or blab on chat rooms about your exploits).

For example, last year it is believed that the North Koreans used a botnet to zombify thousands of computers in South Korea for a DDoS attack that lasted ten days. More recently, two conservative South Korean news papers, *JoongAng Ilbo* and *Korea JongAng Daily,* had their databases trashed and websites defaced allegedly by North Korea in retaliation for some smack talking about North Korea's children's festival. The end result of that attack was the infection and thousands of hours to clean the malware out of hijacked computers which led to thousands of hours of manpower to mitigate future threats. There have been reports for years that the North Koreans have trained some cyber warfare specialists (aka malicious hackers, black hats, whatever) to do this sort of attack, but no one knows for sure if it was them or somebody else. This attack was likely used to test out the South Korean digital defenses, bully the conservative South Korean press, and probably to show the U.S. and Korean governments that they aren't so low tech after all. If you stop to think about it, all it likely cost the North Koreans was time, a few tens of thousands of dollars, some cyber arms dealers on the Darknet, and commitment to the cause. I'd say that is a pretty good investment in the time and money lost to South Korean businesses, not to mention the South Koreans getting pwnd by the North Koreans eh?

Builders, Buyers, and Dealers

In my definition of the cyber weapons industrial complex, I mentioned that it is a subset of the much larger military industrial complex and, as such, many of the players from there can be found in this aspect of arms sales as well. If you were to go onto any defense contractor site (like General Dynamics, Northrop Grumman, and Raytheon) you find listings for "cyber warfare specialists" or "cyber vulnerability researcher" which I'm sure knowledge of Python, Fuzzing Techniques, C/C++, or exploit development should clue you in to what they would be doing: developing cyber weapons. However, the "big boys" of the cyber weapons industrial complex are not the only players on the block and there are "boutique" dealers that are giving the traditional stalwarts a run for their money.

As in any industry, there are the "big boys" and the "little guys" and, usually in the typical military industrial complex, the "little guys" don't do too well. But in this era of "cyber warfare," the smaller players might just have the bigger guns. Last year, during the "year of pwnage" (what we know as the year 2011), Anonymous pulled the shorts down on the computer "security" firm HB Gary Federal and released all their confidential emails online. The treasure trove of documents showed price listings of weapons pages and the clients who they worked for. One of the firms named in the HB Gary hack was an unknown firm called Endgame Systems which was founded by a gentleman named Christopher J. Rouland, better known by his handle Mr. Fusion. Endgame is one of many companies such as KEYW and Immunity that develop cyber weapons for the Pentagon and "other" clients such as the U.S. Chamber of Commerce and other corporate entities. However, this industry is not just an American venture. It is a global enterprise that has other cyber weapons manufacturers in various countries. Of course, here comes the whole issue with the cyber weapons industrial complex: the buyers.

Previously, I mentioned the HB Gary hack and the public release of the confidential emails between HB Gary Federal and Endgame. However, the scariest part of the whole thing was that it was not just the U.S. government buying Endgame's wares, but also American corporations and their "lackeys" on K Street and other shady places. As with the traditional military industrial complex, profit is the true motivation of developing weapons and the same thing prevails in the cyber weapons business.

Back in the 1990s, Arnold Schwarzenegger and the sexy Vanessa Williams starred in the movie *Eraser* about an arms manufacturer selling advanced weapons to some unfriendly (and stereotypical) Russian Mafia dude. Minus the cheesy plot, the idea of weapons being given to a non-governmental entity was the issue for Arnold and the same issue applies in the real world as well. In the physical world, national/local laws, international treaties, and arms embargoes prevent weapons from getting into the hands of the wrong people (sometimes), but in the virtual one there are no such restrictions. Because cyber weapons are not per se weapons, they occupy a gray area where regular laws and oversight allow cyber weapons to be in the hands of some rather unscrupulous folks.

Now, of course, "cyber weapons" can be found anywhere depending on what you want, but when you read through the HB Gary emails, you can see the collusion between the cyber weapons industry, corporations, and their conspirators. The liberated emails from Anonymous showed that HB Gary and two larger security firms - Palantir Technologies and Berico Technologies - were deeply involved in the preparation of an aggressive and possibly illegal attempt to target and silence supporters of WikiLeaks and the U.S. Chamber of Commerce. As in the "real" world, the use of "legally" purchased arms can easily be turned back on the friendly populous to suppress or intimidate them into complying with a certain agenda.

So What?

The reason I wrote this article is to inform our community of weapons and an industry that tends to operate outside the scrutiny of the general public under the guise of "national security." Cyber weapons are not new, but the people who build, buy, and use them are in new territory. Since the advent of the Internet we all are fond of (from, say, 1975 forward), viruses, botnets, and other Internet shenanigans have been confined to mostly the IT or hacker realms. With the "publicity" of the Internet in the mid 1990s, the general public, corporations, and governments have become assimilated into the IT world on some level.

With the amount of information (public and secret alike) on the Internet, the viruses and other malware that was once a novelty for geeks is now not just an annoyance, but a large risk to more people. While there were always people like the one from the movie *Hackers* (folks more focused on profit and selfishness versus being community minded and working for the common good), I'd like to think the majority of us are just guilty of the crime of curiosity, self expression, and being advocates of free speech in pursuit of the intellectual advancement of mankind. However, we see hackers working to make a profit by militarizing malware and root-kits for the military and whoever has the money to buy them.

I'm not hatin' on the folks who work for the companies or founded the companies that are the cyber weapons industrial complex. But think about what you're doing. By enabling governments with people who don't understand technology (past the sensationalist coverage and scare tactics from arms dealers), the ability to easily pwn a hostile botnet is easy, but what are the second and third order effects of that action? I personally think instead of arming them with cyber weapons, we should arm them with knowledge. Call me a "peacenik" or "hippie" but I'd rather make love than cyber war any day.

Thanks to Dragorn whose article "Real 'Cyberwar'" in 28:2 inspired me to do more research on the topic of cyberwar and, more specifically, cyber weapons.

Works Cited

- Coleman, Kevin G. "Department of Cyber Defense: An Organization Whose Time Has Come! http://www.technolytics.com
- McBurney, Peter and Rid, Thomas. "Cyber-Weapons." *Rusi Journal* 157:1, 6-13. http://dx.doi.org/10.1080/➥03071847.2012.664354
- Riley, Michael and Vance, Ashley. "The Code War." *Bloomberg Businessweek,* July 25 - July 31, 2011
- Keane, Bernard. "Anonymous Versus the Arms Dealers of the Cyber War." www.➥crickey.com/au

<?xml version="1.0" ?><title>

XML Automated Gambling

</title>

by Andy Phillips
andyphillips99@gmail.com

Note: This is not a hack or an exploit as such, just a way of bypassing the entire "front-end" of an industry to see how it behaves in pure data format. This is for educational purposes only. Please do not recreate anything in this article.

For those of you out there who are interested in how things work... online casinos are a huge area of interest. Their systems must be able to provide genuine odds of winning whilst continually ensuring reliable company profits - and remember, obtaining truly random results is in itself a very tricky and interesting field.

This article is a brief story about an observation I made, followed by a series of discoveries, tests, and experiments. I thought the results would be an interesting read. Just make sure that you get permission if you do choose to recreate anything described in this article....

Observation

So I was poodling around on some casino flash games on a well known online casino. You can play these games in demo mode, where the odds are produced in exactly the same way as the live games, but with virtual cash. You get a virtual balance of £2,000 assigned to you when you start a session - and this will go down until it hits zero, then reset.

I loaded a slot machine game in demo mode, pulled the virtual lever, and watched some nice graphics followed by a winning message. I had won less virtual money than I had put in. Woohoo!

Using Google Chrome's "inspect element" feature, I clicked on the "network" panel, which shows all HTTP requests between the browser and the server. Unlike FireBug (although I love it), Chrome's feature also includes requests made by Flash - which is what we are looking for.

Here's part of the request URL:

```
/games?random=1330981573957&
➥event=Spin&gameSkin=TikiIsland&
➥numberOfCoins=1,1,1,1,1,1,1,1,1
➥,1,1,1,1,1,1,1,1,1,1,1&coinSize
➥=0.1&partnerId=5&autoPlay=
➥false&playMode=GUEST
```

I then expanded the network request, which was a simple GET request with a query string (although some other online casinos I've checked since use POST). I pasted the URL request in my browser and was pretty surprised by the result:

```
<Events>
<ShowGameReferenceEvent game
➥Reference="0"/>
<DisplayReelsEvent>
<Reel id="0">...</Reel>
<Reel id="1">...</Reel>
<Reel id="2">...</Reel>
<Reel id="3">...</Reel>
<Reel id="4">...</Reel>
</DisplayReelsEvent><DisplayWin
➥Event balance="1998.60" coin
➥Size="0.10" grossWin="0.60" net
➥Win="-1.40" wager="2.00">...
➥</DisplayWinEvent>
</Events>
```

I haven't included the full XML response, but basically it contains all of the game information in clear text: which symbols should show in each position for each reel, what the balance is, what the gross win is, the wager, and which lines won which amounts of money.

I then realized the deceptive issues with these slot machine games:

1) All of the slot machines in this casino use the same API; they just have different graphics, marketing, and jackpots.

2) If you reach a bonus round, the bonus rounds are highly deceptive.

Let me just elaborate on that second point....

It was this particular feature (bonus rounds) that really caught my interest, as this is where you can apparently win the jackpot, displayed at the top of the game and constantly increasing into the tens of thousands. If you reach the end of this round (by apparently choosing the correct items consecutively), you are then confronted with just five boxes to choose from with the jackpot displayed above. So the odds are presented to you as a one in five chance of winning it, which seems almost feasible because it would take a lot of time and money to actually reach this point. Needless to say, after choosing a box I didn't win the jackpot, and when I looked at the XML workings of this process I was very surprised.

When you activate a bonus round (which is totally decided on the server side, remember!), the XML response includes a "bonus round" detailed journey of *exactly* how it's going to play out next.

```
<Pick type="WIN" value="15"/>
<Pick type="WIN" value="45"/>
<Pick type="WIN" value="30"/>
<Pick type="WIN" value="100"/>
<Pick type="RETURN" />
```

So, when confronted with a choice, I could pick *any* object and know I was going to win 15 pence, then 45, then 30, and so on - then fail and be returned to the game.

In other words, the "free" multiple choice element was an illusion. The probability calculation (as far as I can tell) takes place on the server and the game is pre-played for you to eliminate further server calls. The only issue I have here is that the odds are displayed as one in five or one in three on the UI, but actually could be anything!

Onward To See What We Can Do Next

So, obviously the casinos make massive money by offering appealing graphics, animations, and false representations to make you think you are close to winning big. But are you?

I decided since I now had a GET request and an infinite balance, perhaps I could automatically play these games in vast numbers and check out the data afterwards.

I thought I would write PHP scripts to record data into MySQL databases to test out scenarios... like what would happen if you buy a thousand £1 scratch cards (overall loss of £350ish, biggest prize was £100) and which gambling techniques work best (too much to write in this article!).

Because the casino in question here wanted to remain anonymous, I've omitted parts of my script that would identify them and replaced it with notes. An experienced PHP developer would have no problem further developing these scripts to test gambling tactics against games online. Bear in mind, my example was using GET and not POST.

Script

Here's a quick overview of how this works. We use CURL requests, specifically so that we can send a cookie (you can also use CURL to POST). We need to send a cookie, otherwise the demo balance will reset on every move due to a new session.

Then we set up a loop to run for each play, say 1000 plays (whatever you like), build the request, then analyze the XML response, and log or write the data.

```
$i = $plays; // number of plays
while($i > 0) {
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_
➥RETURNTRANSFER,1);
  curl_setopt($ch, CURLOPT_
➥COOKIE, "***COOKIE DATA GOES
➥ HERE***");
  curl_setopt($ch, CURLOPT_URL,
➥ "***BUILD URL REQUEST
➥ HERE***");
  $xmlData = curl_exec($ch);
  curl_close($ch);
  $xml = simplexml_load_string
➥  ($xmlData);
  // Pull results from the XML
  $win = $xml->ShowGambleResult
➥Event[grossWin];
  $balance = $xml->ShowGamble
➥ResultEvent[balance];
  if($win > 0) {
    mysql_query("INSERT INTO
➥ results (result, balance,
➥ wager) VALUES ('WIN', ".
➥$balance.", ".$wager.")");
  } else {
    mysql_query("INSERT INTO
➥ results (result, balance,
➥ wager) VALUES ('LOSE', ".
➥$balance.", ".$wager.")");
    }
  $i-;
  }
```

Simple, huh? Make a CURL request, get the response, dismantle the XML, read it, action it.

I'm sure most of the casinos out there return pretty clear XML, and it's easy to take this apart using SimpleXML. You could even simulate human behavior with random delays and include a user agent definition to further emulate human play. One could easily adapt this script to play roulette, blackjack, slot machines, or any number of games, and record statistical data or try out computational betting techniques.

If anybody does "beat the casino" using such methods, donations are always welcome.

FUNDAMENTAL INTERACTION

Guidance

Dear *2600:*

I just recently came across the HOPE conference website after reading some of the latest news on Julian Assange. I live in the New York City area and wasn't aware of this conference which interests me. I don't know much about hacking and computer security in general and don't have any friends who do either. I was wondering what's the best way to get in touch with people who do? For example, some websites, forums, people, books, etc. I am a curious person and like to learn about various things, but I also had some questions about website and phone security, government surveillance, hacktivism, and related subjects. I have read some articles and have a few books in a list to borrow from the library, but sometimes it's easier to learn one on one with a person who knows about these things. I also am wondering if it's possible to get some advice on web security. For example, I'd like to set up some websites, but am worried about potential problems and might need to hire someone to help. I contacted the hackerspace in my local area, but they don't really do much computer-related stuff. They focus more on building things, which is also interesting.

I'd like to learn more about various other related subjects, such as a low tech approach to computing and the Internet, ham radio, and other things. I hope this doesn't come across as a weird "request" from a stranger. To use a metaphor, I'm not too car-savvy either and there's only so much you can learn on your own by watching videos and reading books, as the auto world is complex and diverse, just like anything in life. So, talking to a hopefully honest and friendly mechanic can help. I also realize people are busy and have lives to live, and some get paid for their work, so I don't want to just bog someone down with lots of questions. I probably will think of stuff I left out after I send this, but that's the gist of it. The upcoming conference interests me, but I'm not sure I'll be able to make it as I have a limited budget for other plans around the same time.

Alex

Obviously, attending the conference would have been a gold mine of information for someone in your position. Hopefully, you managed to make it and learn something about the myriad of hacker-related topics that were on display. If not, make a point of showing up in two years, unless you feel like traveling to one of the other hacker events held around the world. In the meantime, the local 2600 meetings are a great way to become involved and to find people with similar interests. It's all very informal, so you don't have to worry about qualifications, being accepted, etc. It's not something that happens overnight, either. Getting to know people, learning strengths and weaknesses, developing interests... these are all things that take time and patience. Rather than approach this as someone who needs help and advice from people who know a lot, consider what it is that you can bring to the dialogue. Everyone has some bit of knowledge or perspective to contribute and it's highly unlikely that you're an exception. Regardless of how little experience you may have, you'll be accepted as an equal there.

Dear *2600:*

I am a 16-year-old who is currently reading your magazine. I consider myself an advanced user (compared to most), but would be considered stupid by many in this field. I read the Kindle publication and, while I find it interesting, I don't possess the background for utilizing/exploring this field. Essentially, where do I begin? I understand that the Internet is full of such things, but it is bogged down by people only interested in phishing Facebook. I also don't have access to the *2600* meetings. If you could help me or direct me to someone who could, I would be much in your debt.

TheAlpacalypse

There is always the option of starting meetings in your area if they don't already exist. We guarantee there are more people interested in these things than you think. Guidelines are in the meeting section of our website. While there is certainly a lot of stupidity on the Internet, you cannot dismiss it outright as a means of finding intelligent people who share your interests. Like anything else, you

have to do a bit of work to get what you're looking for. This is the theme you should get used to - figuring out the answer rather than simply asking for it. One other notion you need to get out of your head for your own sake and those who will follow you: not knowing as much as others doesn't make you "stupid." If you believe in such labels, then you will live by them. Otherwise, remember that you're in a state of perpetual learning and that you're always ahead of some and behind others. Talk to them all as equals and you'll learn more than you ever thought possible.

Dear *2600:*

I wrote an article I would like to submit to *2600,* and I'm wondering in what format I should send it. There is a bit of code included in the article that should be formatted as such, and I'd like to include an image as well.

xnite

ASCII text is always best for the actual article and, if there are formatting conventions you'd like us to follow, you can always include a copy that demonstrates those in a different format. The less hoops we have to jump through, the more the chance your article will be considered.

Dear *2600:*

I can't help but thank you for how much of an inspiration you have been over the years. Especially when it comes to just letting the professionals do their job.

Shortly, you will be receiving an invitation to download a free copy of my new online zine. I think it will be of great interest to fellow reality hackers. I have even included a very special puzzle along the lines of the sort I suspect would be popular at your HOPE convention. I greatly appreciate any help or suggestions you can offer for getting into the publishing game and helping to get this project off the ground.

Better hurry! You can only download for the next 72 hours.

D

OK, here's a great suggestion we can offer totally free of charge. Don't do what you did above if you want to be taken seriously. You've signed us up to a service that will no doubt keep checking in and annoying the shit out of us. Expecting people to take you up on any sort of unsolicited offer within a strict time limit is presumptuous and, in our case, completely unfeasible. Why not simply send us what you want us to see, instead of expecting us to download something within a brief time frame? Then we'd be discussing what you put together, rather than critiquing the manner in which you tried to share it.

We hope that helps.

Assorted Info

Dear *2600:*

Suggestion for storing back-issues of *2600:* I use 7.5 ounce Cheez-It boxes. Using an angle cut down the front/back and across one side makes for easy access. You can even cover it with decorative paper to match your personal style. Though not incredibly sturdy, they more than meet my needs.

I first heard of this solution many years ago right here in this wonderful magazine.

Rudolph

Sometimes, certain bits of information bear repeating.

Dear *2600:*

Hi guys. I think I've been hacked and everyone on my contact list got sent an email. Don't open the link in the email. I haven't tried it, but I caution against it. Sorry about that.

Alynn

No need to apologize. The email you sent to alert us to this was cc'd to your entire contact list and we harvested dozens of internal email addresses for various corporations and government agencies that you're apparently connected to. Your original email must have been filtered, since we never even saw it. But this one screamed out at us.

Dear *2600:*

Wondered if any of your eagle-eyed readers noticed this from Steve Jobs' biography (by Walter Isaacson) concerning the launch of the Macintosh around January 24, 1984.

Of course *1984,* the George Orwell novel (from where I believe your editor took his nom de plume), and the year your excellent periodical began. But note on page 168 when the launch takes place, "the 2,600-seat auditorium was mobbed."

1984, computer(s), 2600... nuff said.

James

Sometimes numbers and events simply line up randomly in a meaningful way. Just like on TV.

Dear *2600:*

I had to write because I ran into something I thought was neat. I am a ham operator. I bought myself a Yaesu FT-817ND low power transceiver. The manual was barely useful, however there was an optional manual that I bought. This one was written by a group of hams who had bought the same unit and dismantled it both physically and software wise. By their doing this, they found a whole lot more things the radio could do that were not listed in the owner's manual. Are these operators considered hackers? Personally, I think so. How many hackers are ham operators? How many ham operators are hackers? It seems to me that these two groups should be able to get together and communicate. In my case, I have a subscription to *Popular Communications, Monitoring Times,* and to *2600: The Hacker Quarterly.* Just recently, there was an article in *Pop Com* (June 2012) about the Davis weather station and how to set it up and use

it. In *2600* (29:2), there was an article on the same system and how to set it up for hourly reports. I don't know if this was planned, but it sure was neat.

Keep up the good work and a great mag. I really enjoy it. Every month, I wait for my new *Pop Com* and *Monitoring Times* to come in. But not as patiently for *2600*.

616 Boomer

Being that we come out only every three months, we really must be trying your patience.

Dear *2600:*

I have been a reader of *2600* for years living in Flint *Township* (not Flint; yes, there is a difference). There is a Barnes and Noble store nearby. Although presently a subscriber, I do still look for *2600* on the shelf. In issue 29:2, there were a number of letters lamenting the lack of issues present in the Barnes and Noble stores. For at least this one location, I can attest and affirm (lawyer talk for I personally saw them) for the week of 7/9/12, there were current issues present. Others noted that, at times, the issues were covered by other magazines. I agree this happens and all it takes is for one person to screw up the organizations.

Charles

As a publication with many enemies, this is indeed the likely scenario as to why we sometimes get hidden. Fortunately, our support network is far bigger.

More on Meetings

Dear *2600:*

As requested from your website, I am sending an update on how our meetings are going in Charleston, South Carolina. For the past six months, I have consistently shown up at 5:00 pm to the location indicated on the meetings page of your magazine. I have yet to find anything remotely resembling a *2600* meeting.

I don't know how my involvement in the hacking community has gone from speaking at ToorCon to spending Friday evenings sitting alone at a Chick-fil-A. It could be because I'm a pathetic loser.

Regardless, I thought maybe you could update your meetings page to indicate that no such *2600* meetings are taking place in South Carolina. I'm getting tired of eating fast food poultry by myself in a mall.

I look forward to being ridiculed in your editorial response.

Low-res

We actually want to thank you for filling us in. As yours was not the only such report, and since we haven't been getting updates from this location, we've removed it from the listing. Hopefully, a new one will start up in its place. And don't feel bad that you've been all alone at Chick-fil-A. We understand their popularity has gone way down lately.

Dear *2600:*

I am interested in attending one of the Washington State Convention Meetings. However, the Seattle website has not been updated in a long time. I was wondering, does the Seattle group still meet at the Convention center?

Ellie

We have confirmation that this meeting is indeed taking place. The website, though, is in dire need of updating or replacement.

Dear *2600:*

I attempted to join a meeting in Seattle, but was unable to find the meeting room. If the group still meets, what is the room number?

Sean

There's no room number. The meetings take place on the second floor, under the escalators where there are tables and chairs - and presumably a bunch of hackers.

Dear *2600:*

Is this an automated response or a real person?

Sean

Neither.

Dear *2600:*

I've been reading your fine mag for two thirds of my life. I've attended several meetings, sadly long in the past, at the Mall of America food court location in Minneapolis, Minnesota. Even shot you a payphone picture in Conakry, Guinea a few years ago.

Having been in Monterey County for the last few years, I've attempted to attend the meeting listed at the Mucky Duck in Monterey. Three times I've been there. Once I wore my *2600* shirt and walked around the place looking for interesting looking people. I had no luck - just a few random bar patrons.

I went back a few months later and had a similar experience. Despite it being 5:30-6:00 pm on the first Friday of the month, nobody looked to be even vaguely computer-interested. I understand from reading the *Monterey County Weekly* that the Mucky Duck had been shut down for a brief time, and has changed ownership.

The last time was this year. My wife and I went there on time and had dinner. I read my *2600* at the table, asked the waitress if she knew of any related activities or meetings, and she reminded me that the restaurant/sports bar had changed owners.

I would greatly appreciate any further information about the Monterey meeting, as the San Jose and San Francisco meetings are a little too far away. I also fully expect that I'll need to venture further from home to attend another *2600* meeting, as the Mucky Duck in Monterey seems not to be a *2600* meeting anymore.

Just thought you should be aware of the situation on the ground.

dave (aka alphabot)

Thanks for the update. Having received similar reports and not having gotten an update in a

while, we've removed this meeting. As soon as we did that, a new one started up.

Dear *2600:*

I would like to know if there has been any interest in starting a meeting in the Halifax, Nova Scotia area?

Malcolm

Yes, there has been interest, and it's come in the form of this letter. So please start one and see who shows up, then keep us filled in. We would love to have a meeting in that area.

Feedback

Dear *2600:*

Paul Abramson is very right about what an EMP can do ("An EMP Flash - It All Stops" (29:1)), and the extreme general disarray the country would spiral into. My friends and I have been discussing this for a few years off and on, and every time we figure that there is no real solution. The only things that will work are mechanical and monetary, and those will be limited by the minds of the "herd." Good thing we all keep some "mechanical protection devices" around, as they will be the law when all hell breaks loose.

Also, there's nothing like plowing through an entire year of *2600* in one night, though I think I'll be able to find it without fail now that the government delivers it to me. I've always loved that you can get the most "subversive" or "anti-government" periodicals through the mail.

I found "Kill Switch" (28:3) to be very interesting reading, being an amateur radio operator myself. Though I haven't gotten around to it, I'm really hoping that Leviathan didn't use his/her own, or a friend's call sign. Amateur call signs are unique, searchable, and the FCC does have a database containing contact info for each one of us. This could result in a certain amount of harassment, or just some really bright people dropping him/her a line from time to time.

Also, thought you guys might be looking for a bit of a Borders replacement, and I have an idea. Half Price Books is a decently sized chain in the area and they absolutely refuse to censor, according to one of their employees. Think I'll just mention the mag to that employee and see if they can get it from their mag distributor.

Love the mag. Just became a subscriber after reading off and on for five years. One last thing: don't ever stop *printing* hard copy; this e-reader stuff's OK, but paper doesn't need batteries!

E85

We will check into getting carried at Half Price Books. Thanks for the suggestion.

Dear *2600:*

This letter is to expand on what Windpunk was talking about in 29:1 in his article about "Grandpa's Books." For converting to PDF format for "free," you have to look no further than using a Google account. Under the documents section, it gives you an option to convert directly to a PDF file when uploading, as long as the file isn't over two gigabytes. This might mean a little extra work in ensuring the files stay under that limit, but it also means that you can host them in the "cloud" so that you can access them from anywhere you have an Internet connection and Adobe Acrobat Reader.

Just thought I would add that, and Happy Hacking all!

Mickeyshaft

Dear *2600:*

I wanted to respond to Bpa's letter regarding net neutrality (28:3), but I'm mainly responding to *2600's* response.

2600 said, "There's a lot of oversimplification here." I'd agree; Bpa's letter read like boilerplate anti-government rhetoric. Bpa writes, "Government [...] cannot bring about freely made mutually beneficial choice and trades among people." He's correct to a degree, but fails to acknowledge that a proper role of government is to protect these individuals from the initiation of force, theft, etc. In other words, a properly functioning government that upholds the law *will allow* the free market to flourish. I agree with *2600's* point that government is a tool in this regard. Ask not what this country can do for you - nay, don't even ask what you can do for this country; rather, ask how you and your fellow citizens can work *through government* to make this country a better place.

However, *2600's* response revealed its own oversimplification: "[T]he belief that huge corporations will somehow behave in the best interests of the public is the height of naivete." - what level of naivete, I wonder, is the belief that the *government* will behave in the best interests of the public? Pointing out that government can be changed through voting is hardly an answer. It was amusing to see *2600* offer the rhetorical question, "Have you ever tried to use another cable company?" In the 2000 Presidential election, many more *millions* of people voted for Al Gore than for Bush, but we all know how that story ends. I suspect that changing cable companies is probably a lot easier than influencing government to drop some legislation that actually hurts more than helps. Unless, of course, you have lots of money.

With that comment, I arrive at my point - that both Bpa and *2600* are pointing fingers over each others' shoulders when the truth is T-boning them out of their blind spots. The problem is our *government's* sickening willingness to yield to money influence. How ironic that *2600* offered up the example of Verizon dominating all the DSL connections in the neighborhood. *2600* is preaching to the choir on that one; here in New York City, it's either Time Warner Cable or no cable. However, I recognize that the *government placed* that monopoly. What started as an old and misguided attempt to

"protect" a competitive marketplace has turned into a stifling business-government relationship that hurts consumers and gives these corporations more power. Good luck "influencing and changing" that. You won't; there are too many hands in too many pockets. Just for fun, however, I wonder just how much the landscape could change if we tore down these government-placed iron shields protecting the big players.

It is my personal belief that we can keep these big players in check by feeding in the one thing that can hurt them the most: innovation and competition. I don't think net neutrality will work, because as long as the government and big corporations are sleeping with each other, there will always be little loopholes and bribes floating around. However, this is only my opinion and I won't dive into finer points here. My only goal was to point out that this polarized pseudo-anarchy vs. help-us-with-regulation argument isn't going to highlight why anyone needs - or doesn't need - net neutrality regulation.

My sincere thanks for reading my letter - I'm an avid fan of *2600*.

Phil

In the end, the ball is really in our court. When people organize and speak loudly, those in power have no choice but to listen. The recent defeat of SOPA legislation proves this. The problem is that people so rarely use the power that is within their grasp, in all likelihood because they don't believe they actually have it. It's high time that myth was dispelled. It's been high time for a while.

Dear *2600*:

I read multiple rebuttal articles on account of my earlier article titled "The Piracy Situation" (28:4). I don't care to address the articles with much vigor at all. D351's logic that shoplifting helps oppressed third world factory workers is both amusing and representative of the mostly fallacious logic used to rebut me.

What I do want to address is a letter in your most recent issue (29:2), which criticized me for "bending down" instead of opposing legislation such as SOPA, PIPA, and ACTA. I would like to have the opportunity to say that the sentiment is absolutely untrue. While I do believe that the theft of intellectual property is immoral, I also believe that contemporary legislation to combat IP theft is equally (if not more) immoral. I would have hoped that my article expressed that, but I guess it did not. Among the basic liberties that legislation such as SOPA, PIPA, and ACTA violate, the most important are described by - and implied by - the Fourth Amendment. For those readers outside of the USA, the Fourth Amendment of our Constitution reads: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

The spirit of this law is that people are innocent until proven guilty. You cannot demand search and seizure without probable cause because you are then assuming that people are guilty until proven innocent. You cannot assume that people are criminals until they prove otherwise. This is why I refuse to allow the goons at Best Buy, Walmart, and other establishments to look at my receipt as I exit (note that Costco is an exception because I sign a membership agreement that allows them to look at my receipt).

Similarly, any law that allows the authorities to watch what I'm doing online either in real time or by reading logs without a warrant is an unreasonable search. These laws assume that everyone is guilty until proven innocent.

Yes, I believe that piracy is wrong. Yes, I oppose SOPA, PIPA, and ACTA. Yes, I believe that the tactics used by the MPAA and RIAA are wrong. Please don't assume that I'm a weak-minded stooge because I advocate that piracy is immoral.

I don't write this letter to ingratiate myself with the *2600* community. I don't give two rat turds what you all think of me. I write this so that you know that I had really thought about the issues when I wrote my article. My hope is that you'll really think about my arguments instead of dismissing them as the rantings of a copyright yes-man.

R. Toby Richards

Dear *2600*:

The Prophet is wrong when he says that a GSM voice channel is 64Kbps (29:2). GSM traffic may be carried in the backbone network at this speed, but over the radio interface the original voice codec was about 13Kbps and the newer AMR voice codec is variable rate from 4.75Kbps to 12.2Kbps. If you assume that in most conversations only one party is talking at once, we can assume that the average rate is 8-9Kbps. This is much closer to the 3.3Kbps rate of the Iridium voice codec that The Prophet claims. Otherwise a good article.

A point of trivia that wasn't mentioned is that the original number of satellites in the network was planned to be 77, the atomic number of Iridium. However, when launched, it had been optimized down to 66, the current number in operation, so should have been renamed Dysprosium, but wasn't for reasons that remain mysterious. Who wouldn't want a Dysprosium phone?

D1vr0c

The Prophet replies: "You are correct that to conserve spectrum, the AMR half rate codec uses less than 64Kbps over the air interface. It also sounds either like you're using AT&T, talking through mud, or possibly both, but, in either case, considerably better than the quality of voice calls on Iridium."

Dear *2600:*

There was some code I wanted to grab from 28:3. So I went to the code section of 2600.com, only to see that there's no code there at all that is any newer than 2008! What's up with that and when will it be fixed?

grey Otaku

It's yet another item on our to-do list that we unfortunately let slip. We will try to rectify this as soon as possible.

Dear *2600:*

I have to say that it may be a symptom of my age, but the piracy articles (29:2) show quite startling selfishness and ignorance.

I know I could be described as a hypocrite, as you printed my pointers for removing DRM from Kindle publications. Most of these calls to take whatever content you want seem to come from people who have never created anything particularly worthwhile (sorry folks).

I'm not going to argue that the laws are unbalanced and unfair. That's not my point and, to be honest, the constant erosion of privacy in the U.K. is of a greater concern to me, but.... My point is about the people who actually create something and not the free loading execs.

I have had many friends in the music business, some of whom have even "made it" to some extent, but none of them are rich or even well off. The majority of their income comes from mechanical royalties from the song being played on the radio, used in a film, and the like, *not* from record sales

Let's quote jk31214: "Entertainers are already paid for that effort in advance with the option for royalties thereafter." Sorry, but you are not even close to reality! You are paid an advance. *This is a debt*. The artist owes the record company this sum and it is to be paid back out of the 0.07 U.K. pounds received per album sold. Meanwhile, the record company and retailers split the (say) 10 U.K. pound album price (I still call them albums).

All costs, such as recording, distribution, publicity, printing, videos, and travel incurred by the record company are charged to the artist and this comes out of the 0.07 pence per album. The artist also pays for the returns (unsold products) sent back by the stores. Of course, the record companies do not like telling the artist how many albums have been sold. The artist is at the complete mercy of the record company. Additionally, the advance also has to finance actually living - you know, dreary little things like rent, food, and clothes for your kids.

According to Andy Partridge (formerly of XTC), the ideal band would record a multi-platinum album, break up during the second album, and be back working on the building site, unhappy in the belief that the other band members got the money.

Don't point to Spotify, as that alleged recording artist Lady Gaga got paid under 120 U.K. pounds for 1.5 million plays of one of her rancid so-called songs. In the case of Andy Partridge, his back catalog was placed on Spotify by EMI against his wishes (guess which record company owns a share of Spotify) and he can do nothing about it.

What else would you like to know? On old contracts, you only get half royalties for any format other than 12 inch vinyl (yes, that includes CDs).

As David Lowery (in his "Letter to Emily White") puts it:

"Networks: Giant mega corporations. Cool! have some money!

Hardware: Giant mega corporations. Cool! have some money!

Artists: 99.9 percent lower middle class. Screw you, you greedy bastards!"

Yeah, let's unstick it to the man.

Let's keep it simple. If you like something, just buy the damn thing. It's not like it's actually expensive. More blood, sweat, and tears probably went into making it than anything you will ever do (until you have kids, anyway).

You claim to be hackers and independent thinkers. I really don't see where the "I want it so I will take it" is anything above the level of the freaks that appeared on *The Jerry Springer Show.*

So what can you do?

If you wish to destroy a movie company, don't go to see the remakes and encourage everybody you know not to go. Falling demand for those products will stop them from being made in the first place.

Buy from the artists' websites wherever possible.

Just because no physical object is taken doesn't mean it's OK to do so. Somebody worked to make it. If everybody helps themselves to it for free, then the creator won't get paid. Simple as that.

If the majority of movie and record company execs ceased to exist, I would not shed a tear (see Bill Hicks on advertising execs), but without the artists, the world would be a much duller place.

rob

Dear *2600:*

Loved the short story in 29:2. Keep them coming! Liked the writing style and content so much, I'm checking out his book you mention.

pipefish

Dear *2600:*

Hey guys. Big fan of *2600* here. Just sending a quick note to say that I really enjoyed the first edition of what will hopefully be a continuing serial of "geek fiction" in your latest issue. I was skeptical at first, but upon reading I found that I really liked the piece and I think that bringing back serial fiction is a really cool idea; some of my favorite old books were originally published in serial form.

2600 and Andy Kaiser definitely have my endorsement for this endeavor.

Anthony

Dear *2600*:

Yes, please. More Dev Manny stories! Actually, it worked as good marketing: I got his book, which went fast!

Fernando

Dear *2600*:

Re Dev Manny - More of this sort of thing!

cdilla

Dear *2600*:

Re "Firewall Your iPhone" (29:2), the article spreads FUD, is badly researched, and not worth much.

1) It is claimed that "Akamai is a data collecting kind of company." It is not. It is a CDN (content delivery network). Basically, they host files for companies, care about load balancing and having data available close to the downloader.

2) Obviously, the author does not have much knowledge about current smartphone technology, and the author is not good at googling. He claims that "courier.push.apple.com" has to do with Facetime. Well, yeah, as well as any other app that uses push notifications. He obviously did not recognize that the Google results he was getting concerned OS X, not iOS. For iOS, this connection is used for anything that is push enabled. I suspect he forgot to turn off Push Notifications altogether, thus the connections. Oh well.

I do not know if any connections are still made after that point, but I would suppose so, unless even system wide location services are turned off in total. Even then, there may still be a connection coming once in a while to update the current system time.

prattel

Dear *2600*:

Kindle sucks and all the letters in the winter Kindle edition show how aware you are, but yet, even with all of your resources and talent, along with the talent and willingness of your readers, I cannot believe that you support Amazon or Kindle at all. Their practices seem to go against everything you as a publication stand for. I gave them a shot, until losing all of the content I "purchased" due to the draconian DRM issues. I had books that I owned stolen from me by Amazon/Kindle. And an aside, why ebooks at all? Why not just sell copies as PDFs? There are so many better and more functional ways to read content and Kindle and Kindle for PC is about the worst ever. Add in stolen back issues and other content and it seems like a no brainer. I must say I am very disappointed that you continue to have anything to do with Amazon and/or Kindle. I would gladly pay three or four times the price to you for content that I truly own than pay Amazon. Wake up guys and stop selling out. Amazon has made you their bitch. Sorry, but it is so very true and your reply concerning loss of revenue from Amazon if you were to distribute through Barnes and Noble proves just how close you are to becoming total and complete sellouts. I am sure it is more complicated than that, but not out of reach. Hope you come to your senses and stop furthering the creation of yet another monopoly here in Amerika. Thanks for listening to my rant.

Kn@cker7

We can assure you that we're nobody's bitch. This is a new method of publishing and we believe in dealing with it head-on and hopefully helping to shape it into something more palatable and fair to consumers. This is why we speak out about things that are unfair and actually have a dialogue instead of throwing up our hands and walking away - or worse, accepting it and not saying anything. This hasn't affected our publication in any way and we haven't altered anything we do. If that were the case, you would have cause for your accusations. While there are still problems, we're addressing them with those responsible and, having a huge readership on this platform, we're not only educating a whole lot of people, but we're being heard as a major player in the future of ezines. And that "we" includes all of our readers. You don't get this if you don't take part in the conversation. As for alternatives, we're exploring all of them. As of press time, Google has expressed no interest in adding us to Google Play despite our many requests and their willingness to put huge commercial publications on there. Barnes and Noble doesn't respond to our inquiries to add a subscription feature to our magazine on the Nook. Despite your concerns of Amazon and Kindle, they've been responsive and willing to work with us and listen. These organizations are huge and it takes time to get things working the way we want them to. But we feel we're taking some really positive steps in that direction. As for PDFs, we are in the process of converting our entire back issue catalog and we're adding new issues as an annual (and lower priced) non-DRM collection. All of these things take work and time, much more than we had to deal with only a couple of years ago. So we ask for your support and patience as this new way of doing things develops. Please continue to send your suggestions.

Dear *2600*:

One thing I don't understand about the Better Brute Force (BBF) algorithm (29:2) is that it seems to still require iterating through every possible letter combination in order for it to determine valid words.

For example, let's assume a six-letter password length. With a standard brute-force attack, each letter combination of six-letter strings is generated, hashed, and finally compared to the hash. The BBF algorithm also first generates every com-

bination of six-letter strings, then checks validity using the language rules, and finally compares all of the valid results against the hash. In the BBF case, there hasn't been any computing time saved. Instead, the work is being performed at a different step in the process.

This might be effective in the case of generating a list ahead of time to create a reusable wordlist; i.e., a standard dictionary attack. However, given a long enough password length and enough complexity, this task would soon become as unwieldy and time-consuming as the standard brute force algorithm.

Neil (SM)

Dear *2600:*

Regarding "Building a CAT-5 Cable Tap" (29:2), there are two problems with that tap.

First, you will need to make sure you aren't sending into the line. That is hard, but if you are lucky, your network card will negotiate with the switch, believe it's a half duplex line, and stay quiet.

Second, you cause a huge impedance mismatch. In a nutshell, this causes your tap to reflect back part of the signal. Gigabit Ethernet interfaces are often able to compensate for this. They estimate the echo and try to remove it. However, that estimation is then stored in the network interface. It is theoretically possible to read that out and alert the user.

In order to actually make this work well, you'd have to use a high impedance tap. You can try to just add resistors in series, perhaps 1k ohm or more. This will greatly reduce the reflection, but also the amount of signal you get out. It might be too weak for your network interface. Probably the best, but also the most expensive, solution would be to have an amplifier close to the tap. Maybe you can use a modified switch or repeater for this. Be sure to use one which has discrete 100 ohm resistors right after the transformer and remove them.

Casandro

Dear *2600:*

I have been reading your magazine for just under a year, but I'm hooked. I don't know if I can define myself as a "hacker" (for lack of exploits), but I am training for a job in the IT field, studying several technologies, and I semi-understand most of the articles. I read as much for the tone of the magazine as I do for the hope that some of these fine folks' technical knowledge will rub off on me over time.

That said, I was surprised by Feroz Salam's letter in 29:2 regarding an article called "Abuse Reports Still Work," where the author refers to countries that host pirates and otherwise illegal Internet traffic as "smelly." I have to admit that I chuckled when I read that article, and I'm from a third world country myself. I found it funny, and fully in keeping with the tone of *2600,* often sarcastic and sardonic (thus, refreshing).

A couple of points, which I humbly hope will be found of use to your readership:

A. I would not be offended if a person from India (where many hold cows to be sacred animals) told me to my face that a hamburger or a steak is smelly. I'd chuckle and enjoy myself (and I love me a hamburger). If they called America a smelly country, I'd laugh, because it's all a matter of perspective.

B. How many people are offended in these pages who work for Microsoft/RIAA/government agencies? Will *2600* authors stop attacking their bad policies if an offended party from those organizations writes in?

C. Would that be conductive to an interesting body of work? Is it even possible to say something that won't offend anyone? I know a few who find the notion of political correctness in itself offensive, for example.

I love the tone of *2600* and I shudder at the idea that people will begin to self-edit their work to a greater degree than they already do. The one thing I like to do that is hackerish is to think critically, but simply. Keep up the good work, *2600* editors!

Justian17

Dear *2600:*

I was just (finally) reading the Autumn 2011 issue of *2600* and got to the letter from Saskman saying that he was unable to see any images in the Kindle edition. I too subscribe on Kindle and my graphite Kindle DX shows no images whatsoever in your magazine. I had just accepted that that was the tradeoff for getting the magazine delivered automatically on the day of printing.

I too am in Canada, in case that has anything to do with it, and, as stated above, I read it on a Kindle DX Graphite.

If I am supposed to be getting the images, I'd like to see this issue fixed and would appreciate a copy of my back issues with images to be sent to my Kindle or attached to a reply to this email.

Also, in the article "How I Got Firefox to Accept the Tel Tag for Phone Calls" by The Cheshire Catalyst in the Autumn 2011 issue, there are apparently supposed to be tags demonstrating the mailto and tel tag usage. These tags do not show up on my Kindle DX Graphite. Just thought that the editors should know so that this can be handled cleanly in future Kindle editions.

Rod

This is the response we received from Amazon on this issue, which we also printed in the ebook letters section of the Winter issue: "The image delivery is based on the customer's location and the type of device (Wi-Fi or 3G). If the customer is not in the U.S. or U.K. and has a 3G device (Kindle DX), then only one image will be delivered. If the same customer is using a Wi-Fi device (Kindle Keyboard/Kindle 3) and uses a Wi-Fi connection

to download the periodical, then all the images will be downloaded to his device. This is an expected behavior and is due to high delivery costs involved while using 3G." So now that we know that this is their policy, we'd like to hear from readers as to what, if anything, we should do at this point.

Words of Note

Dear *2600:*

Not many surprises were found in the official release of words that cause Facebook profiles to be flagged for review by the DHS, save one. Under the "cyber security" section, the obvious ones are there: "botnet," "ddos," "virus," trojan," and such. But right in the middle of the list was one that gave me a jolt: "2600." I have not sat up in my chair so hard in months.

Wintermute

What can we say? We've been busy over the years building a reputation. This story has really gotten our readers' attention - we've gotten more notifications of this development in recent weeks than all of the (fake) PayPal and (real) LinkedIn spam put together.

Dear *2600:*

It's not like we didn't suspect this already, but you have made the list of keywords and phrases Homeland Security uses to monitor social networking sites and online media for signs of terrorist or other threats against the United States.

Sadly, the entire list has some of the most innocuous things, too. I could mention that I got in a car "crash" and trigger a look-see. Might be even worse to say that I got "sick" from eating uncooked "pork" at a restaurant in "San Diego." For me today, having gotten through the worst of Tropical Storm Beryl here in Jacksonville, Florida, it would be nothing to have a conversation something like this on Facebook:

"Man, the **storm** almost made it to a level one **hurricane** and we had a **flood** in our yard and it ruined my garden **plot**. It rained all night and we had a bad **leak** under the door that left about two gallons of water in the living room. At least it didn't cause the tarp on the kennel to **collapse**. About midnight, there was a transformer **explosion** up at the corner that woke us up. Had two **brown outs** that messed my aquarium filters up and the **power** went out for three hours. Fortunately, I had my little book light and was able to keep my mind off of it by reading *The Best of **2600***. The only good thing out of this is that the rain probably helped the firefighters with the **brush fire** over in St. Johns. Thank goodness we won't need **disaster assistance**."

That's eleven words on the official list of triggers for Homeland Security. I guess I'm on the verge of becoming a "terrorist" or "threat" because I happened to be at the center of Tropical Storm Beryl.

Jen Fone

We wonder what's going to happen when this letter gets transmitted to over 15,000 Kindles.

Dear *2600:*

I just wanted to let you know that it seems that you are doing something right (not that I doubted). A recently released list has confirmed that "2600" is on the list of DHS's watch words. Congratulations on your confirmation. Word has it that you can deliver your acceptance speech at your military tribunal after your "detention" has concluded.

Kathryn

Dear *2600:*

I'm sure you guys are familiar with the data center that's being built in Utah, so I've got no need to explain it any further.

However, something I found of interest was this article I just stumbled across a few minutes ago: The Department of Homeland Security has released a list of words that, when typed into the public feed of a social networking website account that has *not* been set to private (I know, I know, anyone who even buys this magazine already does that, etc., etc.), flags your post for review by the government for possible signs of terroristic content. *You* guys made the list under "cyber security." If I were to type "2600" onto a public update to my Facebook, Twitter, MySpace, etc., that would earn my profile a going over by the Department of Homeland Security for possible terroristic plotting activity. From there, even if I *was* mentioning it in an unsavory context (I would have no need to, but just hypothetically speaking), you can bet my profile just earned itself its own "keep an eye on this guy" file with them "for future reference." I don't need to tell you what this'll mean for freedom; y'all better start watching yourselves - Big Brother apparently didn't like your "ASAT for Dumbasses" articles (personally, I loved reading 'em just for the hell of it). Perhaps I don't know the percentage of terrorist plots that have been trumpeted publicly on Facebook and therefore foiled before they could get out of hand, but I'm guessing it's pretty tiny. I smell something deeper at work here.

Amazingly enough, nothing else well known in the hacking community (like frigging LulzSec, 4chan's anon group, etc., etc.) made the list, aside from a few named viruses and methods of cracking/privacy intrusion. I'm not sure if anyone else has seen and passed it on to you yet, but I didn't want to take the risk that you could miss out. This is completely ridiculous and, in my opinion, un-American (and all that other recycled patriotism tosh).

Not sure if you've featured any articles on that data center, or this website, but it would be a darn good idea to let the information security community itself at large know about this somehow.

Note: I accidentally sent a copy of this email to the webmaster of the *2600* website a few minutes ago, and it didn't occur to me to send it in to the

main news-handling guy(s) until just now. However, you can bet all future activities posted to the website are going to be watched closely too from now on.

M

Just don't feel guilty that it was your email that got their attention. We suspect somebody else must have foolishly mentioned "2600" in an email to the webmaster at some point. And as for that Utah data center, we know all about it and would welcome additional information, pictures, diagrams, blueprints, and the like.

Just Asking

Dear *2600:*

Will there be an option to move a lifetime subscription over to a Kindle subscription? I'd rather be green and have it in a more convenient format.

Matt

At the moment, we have no access to Kindle records (even though for some reason it says publishers do on their website), so we're not able to do anything from our end. We're hoping this changes so we can be more flexible. For now, at least, it's best to think of the print and electronic editions as two separate items.

Dear *2600:*

I've been reading the physical edition of your magazine for over a year now, and have enjoyed every issue. I really want to continue receiving the physical copies, but I'm also interested in the Kindle edition. Is there a "dual subscription" where I could receive both editions for a slightly larger price then a normal subscription? If so, how would I be able to update my subscription (I subscribed via snail mail)? If not, are there any plans for a subscription option like this?

Eric

That's actually not too far off from what you can do now without connecting the two subscriptions. The Kindle version is cheaper than the paper edition so if you subscribe to that one as well, you'll be paying slightly more for the two of them. It just won't all be going through us. If we get access to this feature in the future, we can tweak this more.

Dear *2600:*

Would an article on radio scanning and frequency finding from hotels be of interest?

john

Of course it would! If you think it may be of interest to the hacker community, it's likely many others would as well. Please don't wait for our approval to write articles as we can sometimes take an insanely long amount of time to get back to people. You're always better off having written something than not.

Dear *2600:*

I'm really considering buying a polo shirt from the store but there is no size chart. I don't want to order a large if it is going to be too big! Do you know where I can find measurements?

A. Wolf

We're adding this to our store description so that this isn't an issue. For your convenience, we can tell you that a large has a body width of 23, a full body length of 31, and a sleeve length of 20.25.

Dear *2600:*

I recall that it used to be possible to send you encrypted email... but now I can't find your public key anywhere on your website. What's the deal? Have you given up on confidential communication? Or am I just looking in the wrong place?

dr. ciphertext

Unfortunately, we had to take it down because more than half of the email we were getting that used it was unreadable for one reason or another. It's possible people were using keys obtained from elsewhere that we have no control over or that they were somehow using an incompatible version of PGP. We just don't have the time to troubleshoot every instance where this happens, and the end result is that articles were getting lost, since some were sent from one-time email addresses that weren't checked again. It's unfortunate and hopefully temporary. While many of us have no problem using the means at our disposal, until this becomes easy and transparent enough for the mainstream, it's going to be largely ineffectual. In our case, it started working against us, so we took the necessary steps to fix that. We hope something that works for all clients on all platforms comes along soon and that it's open source and open to scrutiny. Then, and only then, will effective encryption become the norm for email.

Dear *2600:*

I look after the clearances on a two-part miniseries entitled *Cyber Storm* for Sonar Entertainment. Synopsis: When a globe-spanning artificial computer intelligence decides to exterminate the human race, it falls to a team of unlikely heroes to stave off Armageddon.

Our lead actor/hero is a hacker. Would it be possible to have Defcon material for set dressing? Do you have any posters or perhaps Daniel won an award at the latest convention that we could hang on the wall in his apartment? Anything you can provide us to help establish this character would be great. We would of course pay for the shipment of said materials.

Alana

Well, gee. How did you think writing to letters@2600.com had anything to do with Defcon? Do we all look alike to you?

Seriously, it's not hard to check a website and see who you should be writing to. We forwarded this along to the right people as a courtesy. Incidentally, when TV and movie folks ask us for props, we're generally agreeable even if their parent company has sued us in the past. We assume

you don't need anything of the sort from us since we don't see any such request in your letter. That is, unless you asked the Defcon people for 2600 paraphernalia.

Dear *2600:*

Would you be able to change your store to accept Bitcoins? There are various open source applications which keep it up to date with currency fluctuations if that is a concern. It could also save you on merchant account processing fees as it is decentralized.

Further, it would increase your subscription base in areas of the world with slightly more repressive regimes and in other parts of the world would simply provide a payment option more in line with the ideals of our core customer base.

As soon as you do it, I would like to purchase a lifetime subscription.

BB

We're certainly looking into this as a possibility. Yet another interesting development that could wind up changing much of how we do things.

Dear *2600:*

How do I change my mailing address for my lifetime membership subscription?

Michael

The same way you would change your address for a person or utility. Either send us an address change card from the post office or call/email us with your subscriber info. You'll need the info from your mailing label.

Dear *2600:*

I will be overseas soon. How much is extra shipping to APO?

John

This is actually one of the better deals the post office offers. Regardless of where you happen to be, the rates to APO (Army Post Office) addresses are the same as domestic rates. This also holds true for FPO (Fleet Post Office used by the Navy and Marines) and DPO (Diplomatic Post Office) addresses.

Dear *2600:*

I am developing an operating system that is designed to be secure and efficient and was wondering if you guys would be interested in me writing an article on it for *2600*.

Sean

As we've said, it's always a good idea to write an article about something if you think there's a hacker angle to it. It's definitely a great way to get feedback from the people who understand such things.

Dear *2600:*

Sold my Kindle Fire for a Nexus 7. Any news on *2600* coming to the Google Play store?

Kyle

At press time, we have been unsuccessful at getting any kind of response from Google on this. They seem to have no problem carrying the commercial magazines, but when it comes to independent voices, they've been completely silent.

Dear *2600:*

I want to ask if anyone may know how to get Caller ID to identify a blocked name and number. I have a guy who calls our number asking for a person I don't even know. He is a smart ass too. He claims that this person lives at my residence. This fellow is becoming a real hassle. There must be a way to make it expose the name and number.

I want to thank you all at *2600* for putting out a great mag. I am 55 and still play with electronics, but I am a soldering iron type of fellow. I was a nuke for 21 years working with radiation and the associated instruments. I have been a ham for about 30 years now. I am still fascinated with sending a two or three watt signal using CW to bounce off of the atmosphere and communicate with other hams around this planet.

I know this is old news, but it is fun for me. I wish I could contribute some computer hacks and some codes for you. I really enjoy the mag. Keep up the great work, guys and gals. Be safe, everyone, and keep on hacking!

Wirechief

*Different rules apply for different phone companies and it also varies by landline and cell phone. Perhaps the easiest thing to do (we assume you're referring to a landline since you mention a residence) is to block all unidentified calls, at least temporarily. This is called Anonymous Call Rejection and can usually be activated by dialing *77. (To deactivate, dial *87.) This won't let you see a blocked number, but it will force anyone who wants to reach you to unblock their number.*

Dear *2600:*

I wanted to email you an article, but in the latest issue there is no mention of the article having to be in ASCII text. Is this still a requirement or can it be sent in a plain text file? Thanks for your time.

Az

That's what we mean by ASCII. But we will accept any format, as long as we can read it. When that starts to become a challenge, we're more likely to just count our losses and move on. So please only choose formats that are in general use.

Dear *2600:*

Hi, Is this true? Thanks.

A Abdi

OK, let's tackle a couple of things here. First, this writer attached a link, so the question isn't nearly as inane as it looks. But we notice with dismay that an increasing number of people are simply sending us links instead of actually writing things like sentences and paragraphs. Or they speak as if we were receiving a text message rather than an actual letter to be printed. We're not going to start printing tweets, so those of you going down that road can have a very nice trip but we won't be accompanying you. Words are what we're after -

we have the space for lots of them, so please take advantage of that.

Now then, the actual information contained in the accompanying link is rather interesting in the world of hackers and something we can expect to see quite a bit more attention paid to. This was an article titled "Can Your Car Be Hacked?" which focused on the fact that microprocessors direct everything from braking and acceleration to the horn on today's cars. As is standard in such mass media reports, hackers are labeled as the threat to be losing sleep over. If anything, hackers are going to become essential in getting around the true threat. Increasingly, automobile manufacturers are restricting access to components inside their cars so that consumers have no choice but to go to the dealer whenever there's a problem. Independent mechanics are being shut out with alarming frequency because they don't have the right computer codes to get access to the components. Think of the artificial restrictions imposed on our DVD players in the form of region codes and apply that logic to cars. That is what we're facing. The threat isn't from hackers; it's from the manufacturers themselves. However, this isn't being blindly accepted. A "right to repair" law will go into effect in Massachusetts this November and hopefully other states will follow.

So, yes, this is true. Your car can be hacked and, hopefully, you'll figure out how to do it so you can have the access you're entitled to for something that you already own.

Payphones

Dear *2600:*

Thanks for allowing your readers to share this clever way to keep the memory and nostalgia of the payphone alive! Your magazine represents one of our best efforts to continue to make freedom ring (pun intended).

Without taking political sides in the debate, I suggest you are unintentionally undermining one of the greatest and longest lasting freedom debates in the world. In the payphone photo country section, you refer to Taiwan as "Taiwan Province of China." While this would make the folks in Beijing happy, it is a reflection of the very things your magazine has railed against its entire existence.

Taiwan today is a democracy: a free republic. It has a duly elected president and congress, supports its own military, and its citizens enjoy many of the same freedoms as Americans. While there are some who would support a reunification with China (mostly for economic reasons), its people for the most part take great offense at being identified in any way as part of China. While we support and defend Taiwan's existence, ironically we are responsible in great part for helping China foster the rumor regarding its status. Jimmy Carter cast them into their current country without a status when he caved into pressure from Beijing to recognize only one China.

As a result, the United Nations relegated Taiwan to a nonentity. Since that time, Taiwan has lobbied the U.N. on many grounds to establish its existence. China refuses to debate the issue and effectively kills the discussion. However, this is as far as the story goes. China has tried to coerce the world into believing otherwise by referring to Taiwan as its province. This is akin to Fox Broadcasting producing unbiased news or the U.S. government declaring Kevin Mitnick a terrorist.

Since that time, China has tried to force Taiwan into capitulating. However, this tiny nation of 23 million has consistently rejected their attempts. While China could easily win a military takeover, it would suffer considerable loss of life and equal disdain from the world communities. They even prevent Taiwan from using its own name at the Olympic Games and forcing it to be called Chinese Taipei.

These people have endured great suffering and sacrifice to finally be called a nation, only to have the title stripped away. Until their fate is resolved by their own hand, we should honor and respect their choice and rebel against the ball and chain rhetoric of "Province of China" and refer to them simply as Taiwan.

Charles

Seriously, our web page for payphones is not the battlefield for this debate. That page has far more pressing issues at the moment, such as getting pictures of payphones onto it. While this is a fascinating discussion to have in the hallways of the United Nations and various world bodies, all we're doing is using an official list of country names, as kept by the International Organization for Standardization, specifically ISO 3166-1. Getting that list changed should be the priority. Our use of it is apparently helping to spread the word of this controversy, which should be some consolation.

Dear *2600:*

I don't have a "real" camera. Since you prefer "real" photos, would you recommend that I print out these "pseudo" photos? I have some pseudo photo paper that I can load into my pseudo photo printer. I'd rather send .jpg files, but I have found a treasure trove of payphones in Wyoming and I would love to see them published. So let me know what you want me to do and I'll do my best to accommodate you.

Recently Relegated to the Cowboy State

This was actually a very outdated suggestion on our payphone page which has since been removed. Please send your high res digital photos to payphones@2600.com.

Randomness

Dear *2600:*

Long-time reader; first-time writer. After reading the question about host file help by Phillip in 29:2, I decided to break our mutual radio silence with this letter.

Do you ever wonder if you're getting trolled? If I were a troll, I would be salivating waiting to ask about oh, I don't know, my little brother's Japanese Bobtail cat - Mr. Miyagi - who sings in Yiddish (with a Japanese accent, of course) whenever we pair our Sony mobile phones over Bluetooth. Now my Yiddish is rusty, and Mr. Miyagi's Japanese accent doesn't help translation efforts, but I *think* he's singing:

Never gonna give you up
Never gonna let you down
Never gonna run around and desert you
Never gonna make you cry
Never gonna say goodbye
Never gonna tell a lie and hurt you

My theory is Mr. Miyagi won't sing (and thus wake our neighbors) when two non-Japanese phones are paired. My little brother thinks I'm nuts, and I think Mr. Miyagi is nuts, but between the three of us, we cannot find a single iPhone or Samsung or other non-Nipponese Bluetooth device, let alone two.

If I had written with such a trolling question, I know you'd reply with genuine concern and sincere help, perhaps offering detailed plans on how to manufacture feline cranial-foil accoutrements, the further to fill my precious *2600* with rubbish answering rubbish. But, at least I'd laugh as I read your reply, probably adjacent to some Barnes and Noble concern or YALAB (Yet Another Letter About Bindings). And then, as is my custom after devouring an issue, I'd leave it in the subway car or at the Kendall/MIT station for a stranger to find, for a stranger to have his eyes opened to the Hacker Truth and the occasional Letter from a Troll.

Chief Totus and his little brother,
Owens deBrasso

God help the stranger who finds this.

Dear *2600:*

I have purchased the DRM-free content you have recently distributed. I have a quick comment to share. I would not do my parents an injustice, but it's safe to say I grew up relatively poor (but happy). When I got my first computer, I was lucky enough to be able to live near a library which had ample technology titles to keep me busy. My first low-level tech support job was when I started getting into UNIX. A coworker gave me a copy of a popular Linux distro and a CD full of PDFs of actual published books. Was that wrong of him? Maybe, maybe not. It was one of the greatest gifts someone could give me at the time. The point is I wasn't able to afford any of the literature that I was given. This is why today I will go out of my way to support DRM-free and libre documentation. Sure, most readers know how to acquire what they want. Truth is, after you meet authors and grow respect for the community, it makes you feel a little guilty when you don't pay for your content. However, I guarantee you there is a poor kid out there who could quite possibly be the next hacker extraordinaire, and he might not get there because DRM has crippled our ability to help out those in need. I can't walk around with a clean conscious knowing this, and I have enough self respect to be able to look at an author I meet at a con and say, "I bought your book, thanks for that," while knowing if someone needs something, I am free to help them out. Digital Restrictions Management degrades the phenomenon of spontaneous discovery and our ability to help those as motivated - but less fortunate - as us. It really is that simple.

zenlunatic

Generosity and the free exchange of information are investments that often pay off in the form of integrity and further innovation. If we lock those doors, we lock ourselves out as well.

Dear *2600:*

First of all, let me just say how much I love your magazine. I pick up a copy every time I go to my local bookstore and enjoy reading through it. Have you ever thought about publishing an entertainment section? Nothing big, just a little two or three page thing featuring some comics or maybe some reader-submitted jokes, all about technology and hacking, of course. Maybe it could also include such things as small tech quizzes to test readers' knowledge, or quotes from famous computer engineers (possibly written in binary, making it that much more fun to read). I can almost guarantee you it would be an instant hit among the readers. Ask anyone to name a couple sections of the newspaper and their reply will most likely include the comics. Just an idea I hope you will consider. Keep up the good work.

Jon M.

Dear *2600:*

A while ago, I was looking for a career advancement, so I decided to go job hunting at a local job fair. Lockheed Martin was the hottest booth on demand, so I worked up a resume and went to apply. While standing in line, waiting to speak to one of their representatives, the man in front of me, who was also waiting, was having an in-depth discussion about Lockheed's network security infrastructure with the man in front of him. It was very informational and quite interesting.

1. They use VoIP to telecommunicate.

2. All of their network traffic locally and remotely is encrypted with PGP.

3. They used to be running well over 1000 servers, but had recently implemented a more efficient way to save money, energy, and security by installing switches and reducing their servers

down to 150. Having so many servers was causing way too many crashes, bandwidth lagging, and they had to try to patch vulnerabilities and bugs and reconfigure several services which were getting hacked into. All in all, none of their efforts were effective.

4. All changes to their servers or personal computers had to be logged in a log book by hand by the network administrators and previous configs saved on data tapes.

At the time, I had no interest in exploiting these weaknesses and was very impressed at their desire to enforce and create stronger networks. So they were doing what you would expect them to do. So, good job!

E.T.A.G.E.

Dear *2600:*

I'm not quite sure what's going on with the Barnes and Noble bookstores, though I have been noticing something must be awry. Today, I hauled myself out to the bookstore across town, determined to get my *2600* fix. I even joked that if it wasn't there, I'd sit on the floor and stare at the old issue until someone placed the new issue before me. (Yes, I know exactly where *2600* is placed in our Barnes and Noble magazine section. You could blindfold me and I could walk in, bend down, grab the magazine, and check out without a misstep. I've been doing it that long.) I was getting that frustrated. Yesterday (July 12th, three days after the shipment should have been on its way to the store/on stands), I had called Barnes and Noble, asking if they had received the shipment of *2600* (I should also note that they get their shipments on Tuesdays and Thursdays, and as I had called in later in the day, they would have taken stock by then). I was denied, and told to check in next month. For some reason, this sounded really screwy. The week prior (week of July 4th), I was told to check back next shipment day, as it would probably be in soon. My hinky meter was really going off - and I tend to have hunches that end up right. So, like I mentioned before, I went down to the bookstore to just look for myself. And there it was, staring me in the face, the brand new Summer 2012 issue of *2600*. So I bought my issue and went home. I have no idea what on earth is going on here at my Barnes and Noble. They obviously have it and sell it, and I think it's more clueless floor staff that don't rightly care about finding out if I can come in and buy something. For other stores, I'm not quite sure. Perhaps it's time to sit down and write a good old fashioned letter to corporate. A little time and effort on the part of your readers, just to type out or hand write a letter may make a world of difference.

Kamonra

You've likely found the cause of most of the confusion our readers experience, which is simply employees who don't know the answer to something acting as if they do. As with anything else we're told, we should accept it with a grain of salt. This is a far more likely scenario than a nefarious plot of some sort.

Dear *2600:*

I don't know why I haven't seen this suggested before (maybe it has been and I've missed it, maybe it's just not as useful as I think it is), but I believe that switching keyboard layouts could be a useful tool in password security.

Imagine a QWERTY typist used the password "correct horse battery staple". Were they to switch their keyboard layout to Dvorak and type exactly as they usually would, their password becomes "jrpp.jy drpo. xayy.pf oyaln.". A Dvorak typist using the same password but typing on a QWERTY board ends up with "isoodik jso;d nakkdot ;karpd". With a quick keystroke to switch layouts, a plain English password becomes gibberish.

Granted, this is basically a simple character substitution, and a quick script could easily defeat it, but I see no reason why it couldn't become yet another layer of obfuscation to assist in the creation of a more secure password. Furthermore, I just think that there's something to be said for giving anyone reading over your shoulder a hard time.

Keep on keepin' on.

blanuxas

It seems that the person reading over your shoulder would be affected the least by this defensive measure, as they would simply be looking at what was typed, which presumably the typist would also be doing.

Dear *2600:*

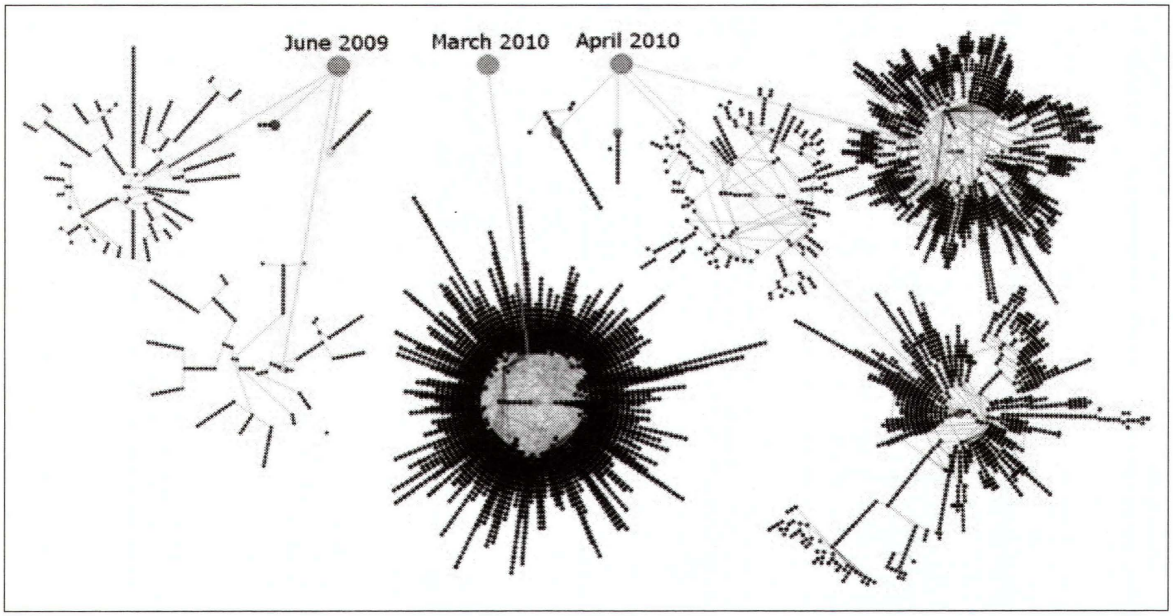
I was just reading through the *2600* cables, and I feel I owe you a big Thank You. I have always been into computers, and recently got a degree in web development. Only recently have I gone to meetings here in Portland. A few months back, I was in a *2600* meeting surrounded by successful folks with great attitudes and great jobs in IT. I decided I wanted to be like those guys. I worked hard, used a bit of social engineering, and landed the best job I have ever had. *2600* brought me to a forum that literally changed my life. My depression, self pity, etc. is gone. I work where I learn all day, and people *constantly* thank me for fixing "stuff" - also, my coworkers love me, as I am stoked to take on simple tasks, which frees up the admins for more important issues. It's a win-win.

I bring a few old school *2600* mags every week and set them near the help desk area in IT. My coworkers in IT read, converse, and chuckle about the good old days. It's spectacular. So, *2600,* I thank you from the bottom of my heart. You were the catalyst for this awesome change in my life. Much love to you.

matt

We appreciate the kind words, but the real credit goes to the community of great people out there. And give yourself some props for being persistent, believing in yourself, and listening.

Stuxnet: An Analysis



by Doug Sibley

The Stuxnet attack is a good case study in what a modern computer virus can accomplish. It is interesting to see how the designers were able to create a program that caused so much alarm, yet only did a very limited amount of real world damage. For Stuxnet to be successful, it had to use a wide variety of tactics, and looking at each of these aspects can give us a good example of what modern threats are capable of.

Attacking the Machine

The main part of any virus attack is a good way to spread it around. With the use of multiple separate zero day exploits, both to infect machines and elevate local privilege, Stuxnet was able to spread itself very successfully. First, let's look at how Stuxnet propagated itself.

Removable Media

One of the interesting attack vectors that Stuxnet used was infecting removable media such as USB drives. MS10-046, referred to as the .LNK exploit, is able to infect a computer when the user opens the malicious folder. By crafting a malicious icon for the .LNK file, a sequence of attack code will run on a machine every time the icon is displayed. For Stuxnet, this vulnerability was used to load the virus from two files also stored on the drive. Using this method, WTR4141.TMP is loaded on the computer, which then executes the main program WTR4142.TMP. Once this has happened, your computer has been infected.

Network

Stuxnet also spread itself quickly across networks, primarily by using two network exploits. MS10-061 is a flaw in the Windows Print Spooler, affecting computers that have printer sharing enabled. By sending print commands pointing to an executable and a specially crafted file, the local machine would become infected. Stuxnet would first send the attack payload in a file called winsta.exe, and then send a file called synullevent.MOF to execute the code. Due to the vulnerability, these files would be created in the %SYSTEM% directory of the target computer using only guest privileges. The .MOF file used to execute the attack would, under certain circumstances, cause winsta.exe to be launched. Normally, .MOF files are used to create and register events and event categories.

In addition to targeting the spooler, Stuxnet could spread itself using network shares with exploit MS08-067. Stuxnet would scan the network looking for c$ and admin$ shares, then attempted to write an attack .TMP file to the remote machine. If successful, a task was also scheduled on the remote machine to execute the payload the next day. Conficker was best known for using this exploit for roughly the same purpose; however Stuxnet had its own

code instead of copying the previous Conficker design.

Using the methods described above, Stuxnet was able to execute attack code on machines its authors wanted to infect. To successfully do this, Stuxnet would need to elevate its privileges when infecting the machine. Stuxnet used two separate zero-day vulnerabilities to accomplish this.

First, MS10-073 was used on any Windows 2000/XP computers. To get system privileges, the exploit uses how Windows handles input from the keyboard to run arbitrary commands at system level. This exploit allows the attacker to modify different DWORDs in a table, then execute a buffer overload against them and run the attack code. Stuxnet used this vulnerability to load system level shell code, which would then install the main Stuxnet virus.

MS10-092 is the second zero-day exploit used, targeting x32 and x64 versions of Windows Vista/7. Windows Task Scheduler allows a user to schedule and execute commands; however, there is a flaw in the way it is implemented. Task Scheduler creates .xml files with the details of every scheduled event, including what permission level to run as. Normally, tasks created by guest accounts cannot use high level permissions. However, this can be bypassed because of the way the .xml files are stored. To prevent the .xml files from being modified, Task Scheduler calculates a checksum for the file when it is first created, and will attempt to recalculate and match before the task is run. Using the CRC32 algorithm, the idea is that any modifications will be found and the task stopped. Stuxnet was able to use weakness in the algorithm to modify the .xml file, and then append a calculated special character to make the checksum match. This allowed the attack code to be executed with the highest privileges on the machine.

Controlling the Machine

Once Stuxnet had established itself on the machine, there were a few other tasks it accomplished as well. Machines attempted to contact command and control servers, initially `www.mypremierfutbol.com` and `www.todaysfutbol.com`, to check in and receive further instructions. Communication between the servers and the machine was done on port 80, limiting the chance that it would be blocked by a firewall. Some of the information Stuxnet would relay back included: OS version/service pack, computer name, domain name, interface IP addresses, and an indicator if Step 7 was installed on the machine. Included in this contact method was the ability for the remote server to send back instructions, such as to stop attacking other computers, as well as a method to update the version of Stuxnet.

To maintain access on Windows machines and to avoid detection, Stuxnet installed a root kit to monitor for removable devices and hide infected files. Called MrxNet.sys, this file had a digital certificate issued by Realtek so that it could be considered a trusted driver and installed silently. After installation, it would monitor directory requests to prevent Stuxnet files from being seen, as well as infecting removable media.

Attacking Step 7

Once Stuxnet had established itself on the machine, it checked to see if Step 7 was installed. Step 7 is the software used to program a PLC, and was the target of the second part of Stuxnet's attack. Using this software, a programmer can create and load the complex programs that run PLCs for industrial machinery, and Stuxnet could monitor and edit the programs.

Stuxnet would first modify the software controlling how Step 7 save files are opened. The objective was to decrypt the save files, then include a full copy of Stuxnet. Once an infected save file was loaded on another computer, Step 7 would automatically load a malicious .dll and infect the machine as well. Once a computer with Step 7 was infected, Stuxnet would also replace s7otbxdx.dll with a malicious version. Since Stuxnet now had full control over the data interaction with the PLC, it could inject specific attack code without the user noticing.

Attacking the PLC

Up to this point, everything Stuxnet had done was to allow the final attack to be successful. Stuxnet was designed to modify a specific PLC, under a specific set of circumstances, and otherwise lay dormant. It is obvious that whoever created Stuxnet wanted to ensure that this PLC attack would be successful, so it is interesting to see what exactly they wanted to do with the PLC.

Before infecting a PLC, Stuxnet first checked to see if it met the requirements. Assuming that it was the correct model, it also confirmed that the PLC was connected to a specific frequency converter manufactured in Iran. If both were true, Stuxnet would then infect the PLC with a

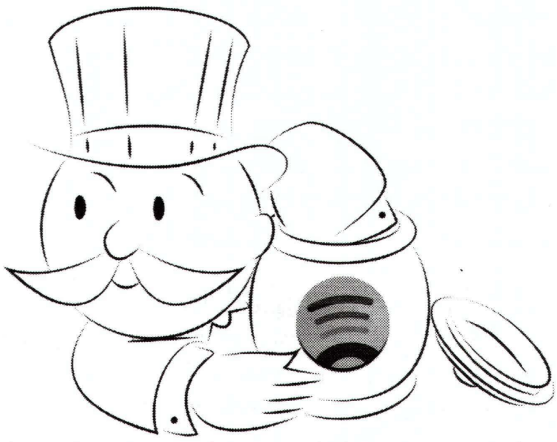
specific instruction sequence. The result of this infection was that the PLC would continue to operate normally, and only sometimes malfunction. Roughly every 27 days, the infected PLC would send the command to the frequency converter to either spin up to 1410 Hz, or down to 2 Hz. In both instances, the speed was well outside the normal operating range and could cause damage over time.

These instructions to spin up or down every month represented the end goal of Stuxnet. It is interesting to note how much concern there was over this virus when it was initially discovered, but in reality it was programmed to cause very unique damage. It is unlikely that anyone other than the specific target of Stuxnet actually suffered any damage from this virus, even though it had infected a large number of computers. Often we think a worm or virus is designed to attack a large number of machines, to form a botnet or other malicious activity. However, Stuxnet serves as a good reminder that this isn't the only option. If an individual or group is able to assemble the technical talent to design a virus and discover new exploits to run it, they can potentially attack any system or process that is run by a computer. As computing has advanced, it is important to remember that the types of attacks that can be carried out have advanced as well. While Stuxnet may have been regarded as the first of its kind seen in the wild, the methodology and ideas behind it are something we will have to deal with for a long time.

Resources

- Broad, William J., and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
- Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier." Symantec Security Response. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. "Stuxnet Under the Microscope." ESET. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
- Talbot, Brent J. "The Journal of International Security Affairs | Stuxnet and After." *The Journal of International Security Affairs*. http://www.securityaffairs.org/issues/2011/21/talbot.php
- Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." Wired.com. Conde Nast Digital, 11 July 2011. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1

How to Leech from Spotify



by Pasikrata

Tools Needed:

- Free Spotify account
- Replay Music software (easily found on the net)

Sources to obtain music for free exist all over the web, as one may well know. Choices range from music torrents to streaming services and music blogs. However, there are times when music fans are unable to locate the music for which they are looking, or are unable to download the music for convenience. This is where Spotify enters the picture and, along with the program Replay Music, performs the task.

Although debate exists about leeching files and can become quite heated at times, we're not here to create any controversy, but demonstrate how simple it is to obtain music from a large source like Spotify and bypass the streaming only service.

Let's get started.

Open up your Spotify program. Then start Replay Music. Your initial step will involve choosing your settings in Replay Music. You'll want to make sure that you choose a decent bit rate from which to leech your songs. A low bit rate won't give your songs the due they deserve. I choose to use the 320 kbps bit rate. Others may choose a different bit rate.

To set up Replay Music properly, go to Settings and choose the Input tab. There you will see a choice of where you want your music files to be saved. I save mine to the desktop so I can get to them quickly and easily. You will need convenience with this as you might need to tag each song. Leeching does take some work, but it is worth it once you have that album you've been wanting for a long time.

When it comes to settings, you may of course choose your own. However, I will suggest the settings I use that I've found work pretty well.

Next, make sure your input source is Audio Driver. Then enter "5" in the Stop Recording After Idle box. It's a good idea to choose "5" as your idle time because with leeching, if you have a song that has a dead space in it, Replay Music will think the song is over and stop recording the song. Five minutes is a good, safe number to use.

Now, click on the Splitting tab. Here, I have the settings as follows: check the Automatically Split Tracks. You don't want to use their default settings, as the settings are not long enough for particular songs with quiet spaces in them. In the Minimum Milliseconds of Silence Between Tracks, I entered in "900". The next box you'll see is Do Not Record or Split Track If Less Than. Enter "500" in that box. Leave the Volume Level Cutoff alone.

The next tab to view is the Proxy tab. Leave this alone unless you use a proxy. If you do, you'll have to make your own settings here.

After the Proxy tab is the Output tab. Under File Name Format, there is no need to enter in your own settings. Leave it as Replay Music has it. Check the Record to MP3s box. Choose your bit rate, and make sure the CBR box is chosen. The Automatic Tagging box should be checked, but this feature does not always work. The recording volume should be in the middle.

We're now all finished with the settings in Replay Music. Let's get on to leeching the Kyuss album we want so badly.

Don't worry about creating a folder for your music as Replay Music does this automatically. You can rename that folder later if you wish. Also, be prepared to play the entire album in Spotify when leeching. Thus, leeching will take a bit of time.

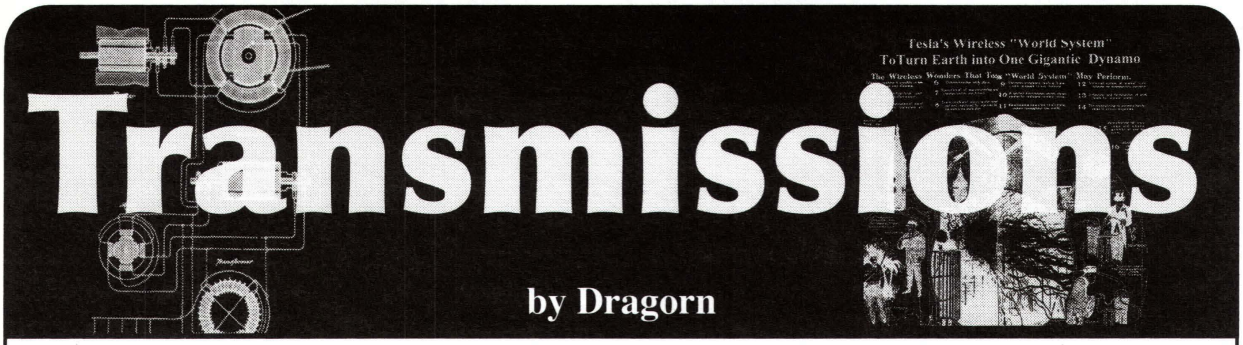
In Replay Music, your next step is to click on the Start Recording button. This gets you ready to record your first song in Spotify. After choosing the Start Recording button, a box will pop up reading, Start Recording Session. In that box, you will want to enter the name of the band as well as the name of the album. This helps Replay Music tag your songs. Choose the Always Tag With Artist Name Above and the Always Tag With Album Name Above boxes and check them. You may also enter the Genre if you wish to do so, but it is not necessary. Do not worry about everything below the Directory Format area. When you're finished with this box, click OK.

You will now see Replay Music recording the first song. Start the first song and permit the song to play completely through. You must watch for the end of the song and click the Stop Recording button immediately after the song ends. This action will prevent you from also recording any Spotify commercials that may pop up during your leeching session.

Now, check your folder where you have it saved and you will see your song there. If you had a commercial come on after your first song, you may see a .wav file. You may delete this file.

Next, do the same with track two on down the line to the end. Be diligent with listening for commercials. Normally, you will have one to three commercials per album, depending on how long the album is. Sometimes, if you're lucky, you may have none at all.

At the end, anyone who chooses this venue has all of the songs they need. Tagging all of the mp3 files that Replay Music did not tag will get files organized properly and ready to transfer to any mp3 player. This is one suitable way someone would leech music files from Spotify.



Transmissions

by Dragorn

Running a Hostile Network

The network at HOPE (were you there? If not, what's your excuse?) presents an interesting set of challenges. It's both physically difficult, because the hotel lacks any significant infrastructure, and technically difficult, because a hacker con is rarely the most gentle of environments. Weird hardware, bored people causing problems, and sheer population density all create some interesting issues.

Physical infrastructure at the Hotel Pennsylvania is significantly limited. While we're fortunate enough to have a wired network which covers most of the Pavillion floor (Floor 2), there isn't much else for a tech conference to take advantage of, which leaves us the challenge of building it all from scratch the day before the conference.

The HOPE network typically consists of about 1000 feet of fiber optic cable, 5000 feet of cat5, and two dozen wireless APs. The exactly layout varies year to year depending on what gear is contributed. For HOPE Number 9, the core network was assembled from Aruba, Cisco, Juniper, and Force10 gear.

The biggest challenge comes from the wireless network. Because wireless is the primary method of giving network access at the con, pretty much everyone who is going to use the network at HOPE (which, to be fair, is far from everyone) is going to be on the wireless. In addition to the wireless network, various areas such as the Hacker Lounge provide wired access. Most of the wired access and project space is on the Pavilion floor.

Wireless is, of course, susceptible to denial of service attacks. Wi-Fi has its fair share to be sure and, even if there weren't denial of service vulnerabilities at the 802.11 layer, it would be trivial to saturate the spectrum with noise. Fortunately, it seems like most of the people who were entertained by this have gotten over the novelty, and generally *deliberate* denial of service attacks are fairly rare.

Unfortunately, Wi-Fi is shared media, meaning *accidental* denial of service attacks happen all on their own, when 500 people in one room fire up their connections at once. The best way to avoid congestion is to move users to other channels. By tuning the access points to try to move people to 5ghz, anyone with a dual-band card should have found themselves on the higher spectrum with more channels free than we could use. However, most smartphones and tablets lack 5ghz support, which gives us no way to get them off the super-congested lower channels.

In 2.4ghz, there are only three non-overlapping channels available (1, 6, 11). If access points are too close to each other, then even those channels may overlap. The network control software figures out how to keep adjacent APs from overlapping, but in an area like the conference room where the main talks are held, all clients will be overlapping each other, causing collisions constantly. Collisions in turn cause packets to be re-sent, which cause more packets in the air, which cause more collisions. It gets ugly, fast.

To try to mitigate the disaster in the 2.4ghz spectrum, there are a few options (and we tried them all). They have various levels of disruption on the network. What works for one conference may not work for others, or may not work the next year, depending on what users want to use the network for. Outright breaking the network for some modes of operation can keep it functioning for the rest of the con.

You can tune the APs to be lower power, so each access point covers less floor space (in theory). When the room is a single large, open room, this won't help much, plus clients will still be shouting at full power, saturating the channels. Access points can be set to drop broadcast packets and multicast packets. This helps (a little) reduce the total packet count on the channel, at the risk of breaking some video streams and other multicast actions.

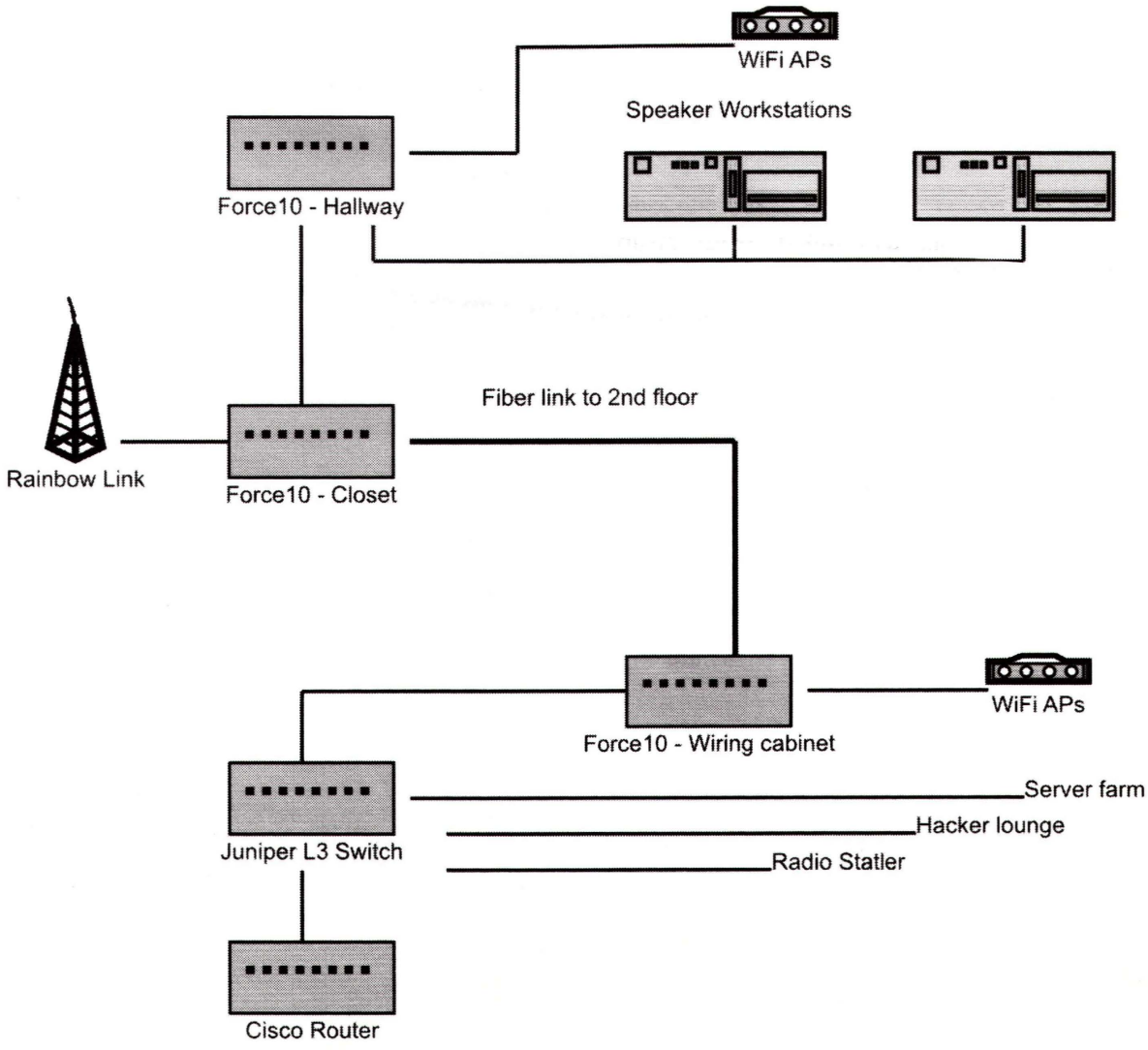
Additionally, limiting the number of users allowed on each access point can increase effective speed. Even though each access point covers most of the conference floor, clients tend to stick to the first one they've seen. By reducing the number of connections allowed on each AP, clients are encouraged to connect to different access points - hopefully the closest one, with the strongest signal. With sufficient

coverage from access points, there's no reason to allow more than 30 or 40 clients per AP. Limiting the signal level threshold also limits the number of clients connecting to an access point. Preventing clients on the other side of the room from connecting can, in theory, reduce interference.

All of these methods introduce minor instabilities into the network. By forcing clients to roam to a new access point, when they otherwise might not, definitely can introduce latency or connection resets, and blocking traffic such as multicast and broadcast can prevent some tools from functioning (such as Apple MDNS auto device discovery). In the grand scheme, however, these limitations allow the network to function at a usable level, when previously it could not. Before implementing these tweaks, the HOPE network saw about 200 to 300 simultaneous users. After enabling them, that number jumped immediately to 300 to 500. The spectrum was so crowded, hundreds of devices couldn't actually establish a usable connection.

Thanks to a generous donation by Net Access (nac.net) of IP space, there were enough Internet-addressable IPs to be able to give them out via DHCP. This meant there was no NAT and no firewalls on the HOPE network this year. This had the double benefit of reducing the load on the network gear (NAT and firewall takes a fair bit of power), making it easier to get cheaper gear to run the network, and it supports the ideals of the conference - the fewer barriers between an attendee and the Internet, the better.

It always pays to remember the environment when deploying a network in a particularly unusual or hostile area, and to also remember the intended use and the reasonable expectations of performance. These decisions would never be necessary on a home network, because they would never be necessary with a handful of devices. For a corporate network, the impact of forcing users to roam more often might not be seen as acceptable, but the range of devices would also be more tightly controlled, allowing for smarter device configuration and capabilities. For a conference, I'm willing to bet being able to get online consistently is the most important attribute, and without mitigation factors, there wouldn't have been much of a network.



RADIO REDUX

by Mr. Icom (Ticom)
ticom.new.england@gmail.com

As an old-school radio hacker from back in the day, I'm pleased to see a revival of interest in wireless topics among the *2600* community. While RF hacking waxed and waned in popularity over the years, there's still a core group of us who pretty much only do radio, and who would like to see more hackers get into it. In this article, I'm going to discuss some basic info for those of you who would like to explore RF hacking, and talk about some of the latest news in the RF hacking scene.

Cheap Receivers

Back in the day, I started with a cheap Electra multiband portable radio that covered the shortwave, and VHF-high public safety bands. It was a tag-sale find, and cost a lot less than a programmable police scanner. A good wideband receiver setup is essential for not only hearing what's out there, but also as one of your first pieces of test equipment to check the quality of signals you might be putting on the air.

If you look around, you could probably find a working CEI/WJ RS-125 setup for a couple hundred bucks at a hamfest, and that would be more receiver than you would know what to do with for a while, both in physical size and capability. If you're really lucky, you might even come across an RS-111, better known as the receiver that made G. Gordon Liddy famous. Radio Shack PRO-2004/2005/2006 scanners, the classic model that got most of us into radio hacking, are being offered at a fraction of their original cost. Most of them already have the appropriate mods done on them. For most beginners though, the most likely entry point would be one of the inexpensive USB stick type SDR (Software Defined Radio) receivers.

All of this started with the introduction of the FunCube dongle (FCD). The FCD is a receiver with nominal 64-1700 MHz frequency coverage (closer to 51.5-2000 MHz, depending on the particular unit) that uses standard sound card drivers under Windows, Linux, or OSX. At ~$175 with shipping to the U.S. (depending on exchange rates), this was up until very recently one of the least expensive ways to buy a wideband receiver.

If $175 is still too much for you, how about $20? It was recently discovered that a USB DTV dongle with an RTL2832U chipset and an E4000 tuner can be used as a wideband SDR receiver with frequency coverage of 62-1700 MHz. At present, this is the least expensive route to get wideband VHF/UHF receiver coverage.

For more information, visit the following sites:

- `http://www.funcubedongle.com` - info on the FCD
- `http://superkuh.com/gnuradio➥.html` - RTL2832U/E4000 SDR
- `http://sdr.osmocom.org/trac➥/wiki/rtl-sdr` - RTL SDR
- `http://zembecowicz.blogspot➥.com/2012/07/worlds-cheap➥est-software-defined-radio➥.html` - even more RTL SDR info, including compiling software under Debian

The Next Step

Hacking RF usually means learning a bit about electronics. Fortunately, the means to do so is available right on the net. Do a Google search for "NEETS Navy Electricity Electronics Training Series" and you will find links to a 24 volume set of PDFs that you can download. This is a complete electronics course used by the U.S. Navy to teach their economic draftees, and it's very good. The other item you should pick up is a copy of "The Handbook," by which I mean that bible of ham radio operators, *The ARRL Handbook for Amateur Radio Operators,*

or more recently *Handbook for Radio Communications*. The material in the *ARRL Handbook* is a little more practical and how-to in nature, and complements the NEETS courses. A brand new current copy costs $50 from the ARRL or your local ham shop. You can find recent used copies at ham radio swap meets (aka hamfests) or on eBay for much less. Any copy put out within the past ten years will suffice, although you might find yourself collecting old *ARRL Handbooks* as the DIY material is different from year to year, and, at less than $10 a copy, you can put together a pretty impressive collection of *ARRL Handbooks* for not a lot of money. The last two copies I bought, dated 1994 and 1979, cost me $1 and $5 respectively.

There has always been a big controversy between the RF hackers who have gotten their ham ticket versus those who remain unlicensed. I've been licensed for the past 28 years, and also have a commercial license since I used to do RF professionally. However, I have to respect the opinion of those who don't want to deal with the geriatric cranktards who often populate the airwaves. I've been licensed since high school, and I'm still considered the "youngster." My attitude is "fuck them." I hang out with all the cool ham radio people instead, and there are quite a few of us. With that said, many of the cool hams are senior citizens with a shitload of practical RF know-how and a willingness to share. They, unfortunately, don't have much longer on this planet, so you should find them and learn what you can while they are still around.

From an experimenter's standpoint, having your ham ticket gives you a shitload of spectrum to play with, ranging in frequency from just above the AM broadcast band to the upper microwave region. Hopefully, soon there will even be a ham band below AM broadcast that promises all sorts of interesting opportunities. Getting the ticket is easy. The questions and correct answers to all of the tests are available, and most people just simply memorize enough to get a passing grade.

While passing the tests is cool, your true education doesn't really begin until you start plying the ether. For those of you who don't want to get the ticket for whatever reasons, there is still a good amount of license-free spectrum you can experiment with. You'll be dealing with Part 15 and Part 95 limitations, but some take it as a challenge. To each their own, I guess.

If you follow ham radio news in magazines like *QST* and *CQ VHF*, you'll find that there is always something neat and new going on. Digital modes using a computer's sound card have gotten to the point where the equipment hears better than you can, and can pull stuff right out of the noise floor. The microwave "weak signal" guys keep going higher and higher in frequency as the equipment for playing up there becomes cheaper and more available.

For the moment now, I'd like to talk about two happenings in the RF scene that are of particular interest for beginners in RF. Both have to do with changes in how the RF spectrum is being used.

Narrowbanding

Narrowbanding is probably one of the best things to happen to the radio hobbyist scene when it comes to the availability of surplus equipment. I expect over the next year or so for the used market to have a lot of neat stuff available for repurposing. Narrowbanding is the implementation of an FCC mandate to reduce the amount of spectrum used by land/mobile licensees, and double the amount of channels available. Previously, LMR systems ran FM with a maximum 5 KHz deviation. The new standard calls for 2.5 KHz. The channel spacing will then go from 15 KHz to 7.5 KHz. All land/mobile radio (LMR) users in the VHF-high and UHF bands must switch their systems to a narrowband standard by 2013. All LMR radios made within the past ten years or so are narrowband compliant, but there is still quite a bit of older stuff in use out there. Commercial radios are built to last!

This means that millions of perfectly serviceable radios will become unusable for LMR use after 2013. While most of them will find their way to developing countries or be scrapped/recycled, there will still be plenty around for hobbyist use. The two meter (144-148 MHz) and 70 cm (420-450 MHz) ham bands are directly adjacent to the VHF-high and UHF LMR bands respectively, and LMR gear can be moved over to the ham bands with no or little adjustment, 90 percent of the time.

The best equipment for the hobbyist would be the 50-100 watt mobile radios, and any radio that is front-panel programmable (FPP). An FPP radio is exactly as described, a radio that you can program frequencies in from the front panel, without the need for a computer with the correct radio service software (RSS), radio interface box (RIB), and programming cable. One of

the biggest differences between ham gear and commercial gear is that ham gear is designed to be set by the user to any frequency within the edges of a given ham band, while commercial gear is set to specific channels in the LMR band, usually by a radio shop, that the user is licensed for. So where a ham can simply tune right to 146.52 MHz for example, a commercial LMR user goes to Channel N and the frequency is pretty irrelevant unless someone wants to listen in with a scanner (assuming the mode is analog FM or P25, and not something like TRBO or NEXEDGE).

Being that LMR users are restricted to specific channels, the equipment cannot be ready programmed to go off their licensed frequencies. Older radios had quartz oscillator crystals in them that determined the specific frequency. Some can be programmed directly from the front panel by entering in an unlock code on the panel's keypad, usually after moving a programming jumper on the radio's circuit board or attaching a programming dongle to the radio. Most radios are done with a computer, using the proper RSS, RIB, and programming cable for the specific make and model of radio. In the days of USB ports, the RIB is becoming a thing of the past with a USB programming cable that goes directly from the computer to the radio.

Of the three items, the RIB and cable are the easiest to get. The RSS may be a different story, however. Some LMR companies are not too bad with software availability, and may have it available at a reasonable cost (or free) without hassle. Other companies are a different story. They may restrict software availability to "authorized service centers" and discontinue software availability for "obsolete" products. Some companies have been extremely aggressive in going after individuals who "pirate" their software. Motorola is notorious for this. Your mileage may vary.

There are also early synthesized radios that are programmed by burning a PROM or EPROM that is then plugged into the radio. The programmers and chips range in availability from unobtainium to pretty common. Generally speaking, the Motorola stuff, using their proprietary modules and "suitcase programmer" such as the MX-350S handhelds, should be avoided as it's almost impossible to get the stuff to get them reprogrammed. The old GE stuff used more common hardware that has since been reverse engineered by hobbyists, and is available in the ham community if you look and ask around.

The easiest and best option for the beginner RF hobbyist looking to get into "real radios" is an FPP model, as no external equipment is needed to get it up and running on the right frequencies. More likely than not, you'll be getting a portable (HT), as that'll be the unit you'll be changing frequencies on most often. There are several types of FPP radios out there. My favorites are the Motorola JT1000, Icom H-16 and U-16, "hamflashed" GE MPA, Kenwood TK-350, and Bendix King LPI (a/k/a U.S. Military PRC-127). If you can find an old Radio Shack simplex repeater box (cat# 190-0345), they work very well with the Icom radios. On the mobile side, a lot of hams like the Kenwood TK-705 (VHF) and TK-805 (UHF). Icom also made the V-100 (VHF) and U-400 (UHF) mobiles that are FPP.

Older crystal controlled radios, in which each frequency is determined by an oscillator crystal inserted into the radio, are generally overlooked by hobbyist types. I've found them a useful source of RF parts, especially when acquired for free. Getting them recrystalled and retuned for ham band frequencies is not too difficult, and they are reliable performers for certain fixed applications where you won't be changing the frequency. Many years ago, I came across a Drake TR-22, which is a vintage solid-state crystal-controlled two meter rig that was recrystalled by the previous owner for all of the AX.25 packet radio channels in the 145.01-145.09 MHz region. It also had the 146.52 national simplex frequency in it, and a couple of other common simplex channels. The radio cost like $30, and it made a very handy packet rig. More recently, I was given a donation of older vintage VHF-low band (30-50 MHz) equipment to help out with a project I'm working on. Included was a Motorola Mocom-70 that was recrystalled to operate on the six meter band (50-54 MHz), simplex frequency of 52.525 MHz. Just attach an adequate 12V power source to the radio, and it's all ready to go. Stuff like this, despite its age, will continue to run like a tank for many years to come. When it does break, you can usually find a scanned copy of the service manual online and fix it with commonly available electronic components, if you can't find someone with a "parts unit" they'd like to offload. If you come across any Motorola MT-500 portables, you might want to give them a second look. There have been

copious ham-related mods done to them, and one gentleman has done a great job converting them for APRS use on the two meter ham band.

That leaves the radios that require computer programming. As mentioned previously, getting RSS can be problematic, depending on the make/model of your radio. Fortunately, there are plenty of hams who work in the LMR industry, and hams who like to work with surplus commercial gear. Assuming you don't come across as a total jerk or basket-case, they will likely be able to get your radio up on the ham bands. *Do not ask them for copies of current production RSS, and do not ask them to program non-ham frequencies into your radio.* I can assure you that the answer will be no, and that future assistance may not be very forthcoming. While hams who work in the LMR industry are, for the most part, very helpful in helping their fellow hobbyists get surplus commercial gear up and running on the ham bands, they're not going to do anything that will jeopardize their job, such as pirating software or putting someone on a frequency they're not authorized for. With that said, some of the older stuff from companies that are not be around in their original incarnation may be available online if you look around. Downloading and using such obsolete, orphaned software for noncommercial (ham) purposes will probably not cause you grief.

My first commercial portable was a Motorola MT1000. They come in a 99 channel variety and, if you find one, you would do well to get it. Those Genesis series radios are true bricks. After that, I ran Saber and HT-1000 portables, which are both excellent radios. Some of the early ASTRO Saber radios are also becoming available in the surplus market, which would be a good way to get a P25 handheld.

For mobile radios, the two Motorola models to look for are the Maxtrac and the Spectra. Both of those have an accessory jack on the back of the radio that, among other things, gives you unfiltered demodulated audio, like a discriminator tap on a police scanner, which can be used for monitoring various digital modes such as POCSAG. These radios will also handle data transmission very well. There are plenty of older Spectras and, to a lesser extent, Maxtracs still in active service. Come 2013, they will not be able to be legally used on the LMR bands.

Some of the best radios to come out of the surplus LMR market are the 100 watt remote-mount mobile radios that also see use as base stations. The radio's control head has a nice small footprint that fits anywhere on a workbench, and the RF deck can be placed somewhere out of the way. Motorola Maratracs are nice, especially if you can get a 99-channel control head for it. The Primo unit in my opinion, however, is the VHF-low band Syntor X9000. Unlike other low-band radios that only cover a portion of the band, the Syntor has full 30-50 MHz. coverage and will operate on both the ten meter and six meter ham bands with up to 128 channels. Syntors have been discontinued for some time now, and are beginning to become like unobtainium. If you find one, grab it and hold onto it!

The Internet is a great resource for ham operators who want to work with surplus LMR radios. Here are a few websites to get you started:

- `http://www.gemoto.com`
- `http://www.repeater-builder.com`
- `http://www.batlabs.com`

Pagers

After seeing my talk on pagers from the original HOPE re-released, it occurred to me that not only was it 18 years ago, but that it was time for an update. I then saw the pager article from the Summer 2011 issue, and was heartened to discover that the topic still had maintained interest among the hacker community over the years. While pagers have been replaced by wireless devices with SMS and email among the general populace, they remain interesting and useful to the hacker hobbyist, especially those who concentrate on RF.

The first thing I need to say is that monitoring pagers in the United States is not necessarily illegal. Pager protocols are not encrypted, and their technical specifics are public information. The law applies to common carrier services, that is commercial paging services, and to radio system users who implement encryption. There exist in the land/mobile radio bands many paging systems that are licensed under the Business-Industrial Land Mobile Radio (LMR) service, and these are fair game for monitoring. Amateur radio operators have also been known to use POCSAG for communications, and monitoring them is fine, too. What may apply from a federal law standpoint is the section of the Communications Act of 1934 that makes it illegal to disclose or take advantage of the contents of an electronic communication intercepted by a third party. There has been

some discussion as to whether that would only apply to common carrier services, or to radio communications in general, but legal discussion of the various communication laws is beyond the scope of this article.

As I've previously mentioned, pagers have mostly been supplanted by SMS and wireless device email. This has had two consequences from the hobbyist standpoint. The first is that the common carrier pager frequencies, at least here in New England, have but a fraction of the traffic compared to the 1990s. The second, and most important as far as this article is concerned, is that there has been an influx of surplus equipment that can be re-purposed for hobbyist experimentation. This is in addition to the POCSAG-friendly amateur radio equipment that has been available for some time. This shows a heartening paradigm shift from simply monitoring systems to hacking and re-purposing cast-off technology to be used for the implementation of hobbyist-type systems, a time-honored tradition among amateur radio operators and other technological hobbyists.

I'll start with the actual pagers themselves. I've seen dozens of these in the bottom of "make offer" bins at hamfests, and I'm reasonably sure that you can probably pick them up for no more than a dollar or two apiece. Usually, ten or twenty bucks will get you the entire contents of a "make offer" bin, and the seller will throw in the bin just so that he or she doesn't have to load it back in their vehicle. The units you want to look for are the 1980s and early 1990s vintage POCSAG and tone pagers on VHF and UHF frequencies. The older tone and numeric pagers, such as the Bravo series, are useful in two ways. They can have their frequency changed to a nearby ham band and be used as actual pagers, or you can salvage the very nice receiver board out of them and use it in another project. From a frequency-changing standpoint, the pagers will be either crystal-controlled or computer-programmable. For those with access to the correct programming software and accessories, the latter are quicker and easier to reprogram. Otherwise, go with the rock-bound boards.

I previously mentioned the Motorola Maxtrac and Spectra. These are readily available surplus, can be easily converted over to the ham bands, and work very well for transmitting POCSAG data. Using these radios is one of the quickest and easiest ways to get a "discriminator tap" for monitoring low-speed wireless data. You will also want to keep an eye out for ham rigs that are advertised as "9600 baud packet ready." This feature is very common in Yaesu and Alinco VHF/UHF ham rigs. Also, keep your eyes open for used Kantronics KPC-9612 TNCs, as they do POCSAG rather well.

For those of you without ham tickets, provided you stayed within the necessary technical specifications and FCC regs, the MURS band can act as a substitute for two meters for your POCSAG system experimentation. All that surplus VHF-high band gear will move over to the MURS channels with no problems whatsoever. The older wideband stuff will need to be used on the wideband MURS frequencies (154.57 and 154.60 MHz), and you will need to crank the power down to two watts or less.

In a similar vein, I was experimenting with some older Motorola Bravo pagers (POCSAG) on the UHF business band (464 MHz) to see how well they would perform when the customer in question narrowbanded their business' radio system. For the test, I used my trusty KPC-9612 into the external modulation (EXT MOD) input of a service monitor. Without any modifications, the pagers were able to successfully decode POCSAG at narrowband transmitter deviation (below 2.5 KHz). In fact, I did not notice any problems with data decoding until the deviation dropped below 1 KHz In practice, narrowband deviation is usually set at 60 percent of the maximum limit. That would be 1.5 KHz in this instance. My recommendation, based on my experiments, would be to aim for a deviation around 2 KHz. That would give you plenty of swing for reliability, while still keeping you legal.

Epilogue

For those of you who really want to get their hands dirty, I have been reading this excellent RF book published by the ARRL titled *Experimental Methods in RF Design*. This is for those of you who want to get seriously into rolling your own gear from scratch. Of particular interest to readers of this article is Chapter 7: Measurement Equipment. Test equipment can be an expensive proposition for the RF experimenter, and this chapter shows you how to make a lot of what you'd need.

There are certainly a lot of cool and interesting things going on in the RF hacking scene, and I only touched on a few of them in this article. If you'd like to see more of this material in the pages of *2600*, please contact me via email at the address above.

Physical Security Threat from Hotel WiFi

by R. Stevens and A. Blum

Most hotels offer in-room wireless Internet service through unprotected, unencrypted access points. Connecting to these access points places your wireless devices and unencrypted traffic at risk of exposure to malicious users on the network. The purpose of this article is to make users aware that their physical security is also at risk when staying at hotels that utilize pay-as-you-go Internet services. This article is not meant to be a "how-to," but is meant to inform consumers about a potential threat and ways to better protect themselves when traveling. The steps detailed below reflect the authors' experience with what appears to be a common hotel paywall application.

Guests attempting to log into the hotel WiFi are presented with a splash pay-page that asks for hotel room number and last name. Once these credentials are verified, they select the preferred type of Internet service and the paywall adds the computer's MAC address to the access list.

Utilizing PortSwigger's Burp Proxy, an attacker can capture outbound web traffic and access paid Internet at a guest's expense. This can be achieved by setting the Burp Proxy to intercept mode and the web browser proxy to Burp. An arbitrary room, surname combination entered at the pay splash page will establish the base HTTP request. This request can then be viewed and sent to the Intruder tab. From Intruder, the attacker can utilize the sniper payload to isolate parameters to the room number and last name form fields. Simple rules can be created for each form field to reduce the amount of network noise and time required to conduct a successful dictionary attack. Room number ranges can be easily gleaned from the placards near the elevators on each floor (e.g. 511 through 549). A dictionary list of the ten most common last names would likely be sufficient for the name field. With this configuration complete, the attacker can launch Intruder against the splash page and the responses can be monitored. A successful dictionary attack will usually be indicated by a vastly different response (in our tested case, it was approximately triple the length). The attacker now can "borrow" the guest's Internet access or take it one step further.

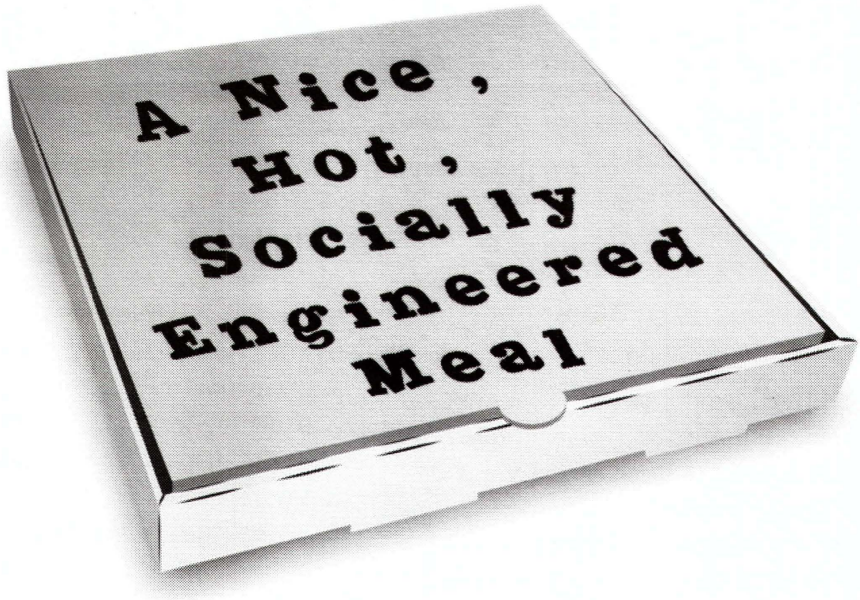
Given the guest's surname and room, it is now possible to obtain room keys using a little social engineering. An attacker can claim a lost or misplaced key at the front desk and request a new key. If the hotel staff requests ID, the attacker can claim that they left their wallet in the room as well. The next responsible step for the hotel staff would be to escort the assumed guest to the room and request photo ID before departing; however, most hotels neither have the staffing available nor the trained employees to ensure the verification happens. Personally, the authors were never asked for identification or personal information verification when attempting to gain physical room access.

We recommend that hotels abandon the simple splash pay-page for an encrypted site that requires a little more personal information verification or a valid credit card number. Hotels should provide better education and enforcement of security policies to help mitigate a majority of the physical risk to hotel patrons.

As of right now, there are no measures in place to protect guests against fraudulent WiFi charges caused by this dictionary attack methodology. Guests should inspect their check-out receipt for any charges that they do not recognize; normally the staffers at the front desk will remove the charge with no questions asked. We recommend that guests assume an active role in their own protection by informing the hotel front desk not to issue any additional room keys without valid identification. They should also utilize the door deadbolt when inside their room and store high-value items in the room's safe.

Safe travels.

Burp Proxy is available for download at `http://www.portswigger.net/burp/proxy.html`.



by Gregory Porter
greg.e.porter@gmail.com

There are a number of options in methods of obtaining food or, in my case, pizza. One can dine in, pick it up, or call in the order to have it delivered - and you can also go online and order it. My recent first experience with GrubHub.com illustrates the power of assumptions on a situation. I suppose the title is a little misleading. Social engineering refers to the practice of manipulating someone to gain access to a system. Here, I refer to the manipulation of assumptions for personal gain. This is, of course, for educational purposes only.

When making an order with GrubHub, one must first make a free account by providing a name, address, email address, and phone number. A credit card is not required. To confirm the order, a payment form must be chosen between PayPal, credit card, or cash. If one is paying by card, a tip amount can be specified. Special instructions for the items or delivery can also be specified (like "knock on the door three times"). Easy, right?

I ordered a two topping, large pizza and jalapeno poppers. With tax and the delivery charge, the bill totaled about forty bucks. I like to minimize the use of my credit card online, so I opted for a cash payment. I also wanted to have to ability to modify the tip, depending on the delivery time. The order was quickly and easily confirmed with an email and, after an hour, the pizza arrived.

The delivery guy gave me the food and started to leave. I asked how much I owed him. He replied that I had already paid. I hesitated. I didn't remember putting my credit card online. I explained that on GrubHub, I chose to pay cash, not with my card.

He looked at my bill and said, "You used GrubHub, right?"

"Yep."

"Normally, when someone uses GrubHub, they just pay with, like, PayPal. But let me check."

He pulled out his phone and called the pizza place. "The order for two topping large pizza for [address redacted] is already paid for, right?"

He hung up the phone and said, "Yeah, it's all paid for."

He was a nice guy. He didn't want me to pay any more and I didn't want to pay for any less. I shrugged, thanked him, and went back inside.

As I ate, I looked at my receipt email. It read "Paid by cash." I suppose that means "I will have had paid with cash by the conclusion of the transaction."

Using a site like GrubHub, the pizza place assumed I would be paying with my card. It is, after all, more convenient to pay like that, so I suppose that's what most people do. This tendency, coupled with the slightly misleading future perfect tense, resulted in a free meal for me!

The moral of the story is that assumptions we make about a given situation, process, or system, whether it be a network or program or human interaction, can powerfully impact the final result. So, be careful about what you assume (especially if you are a pizza guy). Happy hacking!

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 17-21 **(DATE CHANGE)**
ToorCon
The Weston
San Diego, California
sandiego.toorcon.org

October 19-21
Hackmeet
Noisebridge
2169 Mission Street
San Francisco, California
hackmeet.org

October 20-21
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

November 9-11
PhreakNic 16
Clarion Inn & Suites
2227 Old Fort Parkway
Murfreesboro, Tennessee
www.phreaknic.info

November 17-18
Kiwicon 6
Wellington Opera House
Wellington, New Zealand
www.kiwicon.org

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany **(CITY CHANGE)**
events.ccc.de

February 15-17
ShmooCon
Hyatt Regency
Washington DC
www.shmoocon.org

April 18-21
Notacon 10
Hilton Garden Inn
1100 Carnegie Ave.
Cleveland, OH
www.notacon.org

July 31-August 3
OHM2013
Geestmerambacht, The Netherlands
www.ohm2013.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

For Sale

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30, including worldwide shipping. Check out this open source project and more at DangerousPrototypes.com.

GAMBLING MACHINE JACKPOTTERS, portable magnetic stripe readers & writers, RFID reader writers, lockpicks, vending machine jackpotters, concealable blackjack card counting computers, poker cheating equipment, computer devices, odometer programmers. and much more. www.hackershomepage.com

CLUB-MATE is now available in the United States. The caffeinated German beverage is a huge hit at any hacker gathering. Now available at a reduced price of $55 per 12 pack of half liter bottles INCLUDING SHIPPING. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v29no3" and get 10% off of your order.

PRIVACYSCAN FOR MAC OS X seeks and destroys potential online and offline privacy threats with 35-pass wipe. Available on the Mac App Store for a low introductory price - http://privacyscan.securemac.com

BUS PIRATE, our most popular open source project, is a universal bus interface that talks to microchips from a PC serial terminal. Here's how it works. When either you or your software script enter commands into a terminal on your computer, those commands are interpreted by the Bus Pirate and sent via the proper protocol. The Bus Pirate then interprets data sent back to your computer terminal - and you see the response on your screen. Simple! The Bus Pirate is public domain, you are free to rework and reuse this design in your own projects. $30 including worldwide shipping @ DangerousPrototypes.com.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/portable-penetrator-wpa-66c1.html

Help Wanted

ANONPR.NET NEEDS RECRUITS W/SKILLS! All of us over at the Anonymous Public Relations team are working diligently to publish the stories that your traditional media sources refuse to touch. No matter what your skill set is, if this appeals to you, please come visit us at WWW.ANONPR.NET or find us in #AnonPR on IRC.AnonPR.net to enlist your services with us!

CAN'T HACK? Won't ddos? You want to help anyway? Help us here! Get active at wiki.freeanons.org and support the Anonymous Solidarity Network!

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

Wanted

WANTED: AUTUMN 1988 ISSUE of *2600 Magazine* (Physical Copy). I am seeking a physical copy of this issue to complete my collection of *2600 Magazine*. How to arrange payment and amount we can discuss, but I prefer PayPal. Magazine condition is negotiable, provided that it is complete and readable. I will need verification that you have the copy in-hand; photographic proof is acceptable. Having a high-positive feedback rating on eBay, or some other form of trusted and verifiable rating, will go a long way toward closing this deal. Please PM me (cr0sh) at the ElectrTech forums if you can help.

WE'RE ACTIVELY SEEKING SUBMISSIONS for a new print magazine covering a broad range of tech/non-tech subjects, such as: proven physical security techniques, "Breakdown of a Takedown" (dissections of law enforcement attacks), real-life financial privacy tactics, cross-jurisdictional lifestyle tutorials, implementing genuine privacy in the cloud, configuring

private smartphones, etc. Geared to non-specialist audiences, 100% non-profit, & community-powered. Be a part of the first issue - share your wisdom! Info: privatelifestyles@hush.com.

Services

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" study guides make it easy to get your Technician Class or General Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from www.kb6nu.com/tech-manual. E-mail cwgeek@kb6nu.com for more information.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

JEAH.NET UNIX SHELLS & HOSTING. Quad 2.66ghz processors, 9gb of RAM, and TB and TB of storage? JEAH.NET is #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Don't forget our free private WHOIS registration service, with domain purchase, at FYNE.COM.

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensics certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory ads with link to your website to help you expand your business and improve search engine placement. Place FREE classified ads! Search over 35 million classified ads to help you find what you want by searching over 75,000 different social media and online classified ad websites. Thank you for being part of our online audience.

Announcements

SEND A *2600* GUY TO CONGRESS. www.DaveChapmanForCongress.org I am a *2600* subscriber and will try to reduce the cluelessness level in Washington. If you are in Silicon Valley, vote for Dave Chapman.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2011 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

Personal

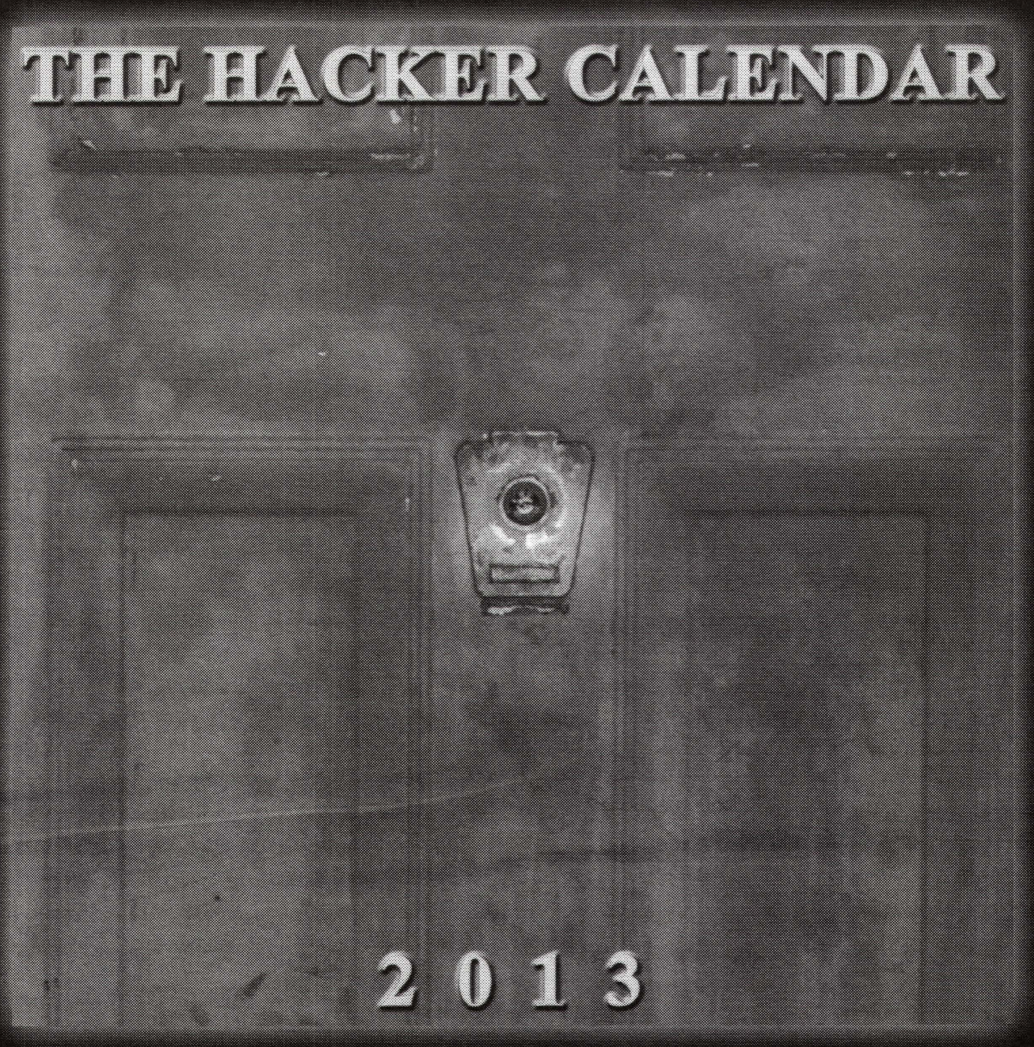
INCARCERATED HACKER WITH LEUKEMIA. Thanks to the few who have communicated their support as we focus towards remission - McGraw especially. Difficult at best currently, with daily chemotherapy treatments with its side effects, including the twenty plus pills keeping myself alive. Trying my hardest to learn Japanese (bucket list) and mend my broken ties. As I undergo continued treatments and incarceration, just a simple letter of solidarity and moral support would be generous. I would appreciate assistance towards my goal of learning Japanese - it's an awesome distraction from the everyday. To everyone, thank you for the encouragement. Look forward. Preston Vandeburgh G66791, California Medical Facility, Post Office Box 2000, Vacaville, California 95696-2000.

FREE GHOST EXODUS NOW! You have no idea how ridiculously uber boring prison is. But you can help me pass the time by being my pen-pal. I respond to all letters. Pics are cool too. I'm into musical instruments, religion and ministry, paranormal, urban/wilderness/virtual exploration, drawing, novel writing, Linux, digital forensics, Anonymous, conspiracy theories, and cyber warfare tactical theories. Hate mail is welcome. Ha! Snail mail me: Jesse McGraw, Reg# 38690-177, P.O. Box 9000, Seagoville, TX 75159. myspace.com/blackfridaynull

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*
Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Winter issue: 11/21/12.

Are You Ready To Plan For Next Year?



Each month has a 12x12" glossy display of surveillance technology at work. (Some of the pictures were taken at great risk!) Nearly every day of the year is marked with updated hacker history.

$14.99 includes domestic shipping

store.2600.com/calendar

"If you only knew the magnificence of the 3, 6 and 9, then you would have the key to the universe."
- Nikola Tesla

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Forum Admins
Bunni3burn, dot.ret

Inspirational Music: Pussy Riot, Snoop Lion, Gotye, Geistform, Peter Schilling, Khaze, MOTP, Childish Gambino, Gummy Soul, Yo-Landi Vi$$er, George Clinton, Yuksek, Tipper, Chris Clark

Shout Outs: William Binney, Deviant Ollam, Steve Rambam, Sick Beard, Hannibal Buress, CO2, Aaron Swartz, Tesla Science Center at Wardenclyffe, teachers everywhere, CERN, Immi, Matthew Inman, JPL, and everyone involved in making HOPE Number Nine a smashing success

RIP: Billsf

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 (ISSN 0749-3851, USPS # 003-176); Autumn 2012, Volume 29 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2011 at $25 per year. (1987 only available in full back issue sets.) Individual issues available from 1988 on at $6.25 each. Subject to availability. Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**
Copyright © 2012; 2600 Enterprises Inc.

MEETINGS

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354

AUSTRALIA

Melbourne: Softbelly Bar, 367 Little Bourke St, Melbourne. 6 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Newk's, 4925 University Dr.

Arizona

Phoenix: Citizen Expresso Bar, 4700 N Central Ave. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: East Village Coffee Lounge. 5:30 pm

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Colorado Springs: The Enclave Coop, 2121 Academy Circle. 7 pm

Loveland: Starbucks at Centerra. 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: Tijuana Flats at San Marco, 5635 San Jose Blvd. 6:30 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Panera Bread, Fashion Square Mall.

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Northampton: The Yellow Sofa, 24 Main St. 6 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Las Vegas: Barnes & Noble Starbucks Coffee, 3860 Maryland Pkwy. 7 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Mexico

Albuquerque: Quelab Hacker/MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: SUNY Albany Transfer & Commuter Lounge, first floor, Campus Center. 6 pm

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 7 pm

North Dakota

Fargo: 222 E Market St, upstairs near the bar, but not in it. 6 pm

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

San Antonio: Bunsen Burger, 5456 Walzem Rd. 7 pm

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Payphone/Booth Alterations

Scotland. Found in Cleish, the traditional red booth that used to be seen everywhere in the United Kingdom has now found an alternate use as a bastion of information. We hope at least there's a phone book in there.

Photo by Sarx

United States. What are the odds of getting two such submissions for the same issue? Seen on Broome Street in New York City, this library is a bit smaller, but with room to expand. Complete with locking doors.

Photo by John

South Korea. Not really a payphone and not really an alteration, but an example of why we encourage submitters not to have humans in the shot. The result here looks like some kind of weird phone creature staring back at us. This regular phone inside a phone booth was found at the Rodriguez Range U.S. military installation.

Photo by Josephus

France. This can be thought of as a doubly foreign payphone, since the traditional red booth immigrated from the United Kingdom and the phone itself is in the French city of Pontorson. In all likelihood, the components came from someplace else, so this represents a real melting pot of telephony.

Photo by Tom

Visit **http://www.2600.com/phones/** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos

We're not going to kid ourselves into thinking that this picture wasn't doctored a bit. We suspect that the total price was $26.00 and the amount of gallons was 6.667. Removing the decimal points and the 7 made this look like a truly "Satanic gas pump," as **Dor Occas** tells us. It's close. The only time that such a numerical lineup would be possible is when the price is $3.899 a gallon (since pumps in this country always have prices that end in nine-tenths of a cent). Now, if someone can find a pump that only shows two numbers to the right of the decimal point rather than three, the amount of gallons could actually show up as 6.66. (We'll overlook the decimal points.)

CAP'N CAPTAIN CRUNCH - Vintage Hard Plastic Bo'sun Pipe - RED & YELLOW WHISTLE
Like
Item condition: --
Ended: Mar 27, 2012 19:43:28 PDT
Winning bid: US $26.00 [12 bids]
Add to list
BillMeLater $10 back on 1st purchase & 6 months to pay
Subject to credit approval. See terms
Shipping: $3.12 Expedited Shipping | See all details
Item location: Dunning, Nebraska, United States
Ships to: Worldwide
Delivery: Estimated within 3-4 business days.
Payments: PayPal, Bill Me Later, Pay on pickup | See details
Returns: 14 days money back, buyer pays return shipping | Read details
eBay Buyer Protection
Covers your purchase price plus original shipping.
Learn more
Top-rated seller
stoolshed (25764)
100% Positive feedback
Consistently receives highest buyers' ratings
Ships items quickly
Has earned a track record of excellent service
Save this seller
See other items
Visit store: stoolshed
Mouse over image to zoom
Sell one like this

Talk about numerical lineups! This one, according to **Barry Mullins**, was a big coincidence. He was bidding for the famous Cap'n Crunch whistle that emits 2600 hertz and this was his winning bid. What makes it even better is that he bid a higher amount and this is what eBay calculated as the final price. It was clearly meant to be.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.